CYBERSECURITY FOR MOBILE DEVICES

A COMPILATION OF INFOGRAPHICS FROM ASEAN COUNTRIES

ASEAN · JAPAN
Cybersecurity Cooperation

Introduction

The increased use of smartphones and other smart devices has made life more convenient. At the same time, it has also exposed us to risk from cyber threats such as online scams and data theft.

With the COVID-19 pandemic triggering a surge in digitalisation and e-commerce, the attack surface for cyber criminals has correspondingly increased. It is now more urgent than ever for government agencies to increase public awareness of cybersecurity and the need to adopt measures to protect our devices and data.

At the First ASEAN-Japan Cybersecurity Working Group Online Meeting on 18 Feb 2021, ASEAN Member States and Japan agreed to work on building cybersecurity awareness through collaborative efforts. This compilation of infographics by ASEAN Member States and Japan based on the theme, "Cybersecurity for Mobile Devices", is an initiative to bring countries together to share best practices and exchange public education resources. More importantly, it aims to help the citizens of the ASEAN-Japan community navigate cyberspace safely.
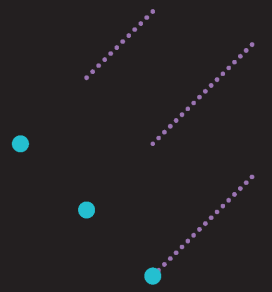
Contents

Brunei
Darussalam

Two-Factor
Authentication

Two-Factor Authentication

or **Multiple Factor Authentication** is when a user successfully presents two or more pieces of evidence to an authentication device to gain access to his mobile device.

Examples of Two-Factor Authentication

Password & E-mail Verification

Password
••••••

+

Hi,
Good on you for keeping your account secure.
Here's your authentication code:
738118
This code expires in 20 minutes, but you can generate another by logging in again.
What to do if you didn't request this email
This email is sent automatically when you log into your MYOB account. If you haven't logged in recently, someone else might be trying to access your account.

Password & SMS Code Verification

Password
••••••

+

Messages
🔍 Search
220-00   6:16 PM >
● G-964261 is your Google verification code.

PIN Code & SMS Code Verification

●●●●●
1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
	0	

+

Messages
🔍 Search
220-00   6:16 PM >
● G-964261 is your Google verification code.

Enable Two-Factor Authentication On Your Social Media Accounts

WhatsApp
Settings > Account > Two-Factor Verification

Facebook
Settings & Privacy > Settings > Security & Login > Use Two-Factor Authentication

Instagram
Settings > Security > Two-Factor Authentication

Twitter
Settings and privacy > Account > Security > Two-Factor Authentication

LinkedIn
Settings > Sign In & Security > Two-Step Verification

Telegram
Settings > Privacy & Security > Two-Step Verification

Apple ID
Settings > [Your Apple ID] > Password & Security > Turn on Two-Factor Authentication

Google Account
Go to https://myaccount.google.com > Security > Select 2-Step Verification > Follow the instructions to turn on 2-Step Verification

Cambodia

Mobile
Password Management

SECURITY

MOBILE PASSWORD MANAGEMENT

Set up unique password / pin / passcode not related to your personal information

Use a password manager to stores all the login information you use

Lock your device with strong password / pin / passcode

Use multi-factor authentication to confirm your identity before you can access an app or website

Use biometrics to unlock your device (Ex. facial recognition or fingerprint access)

Don't share your password to other

Use unique and separate password for each account and app on your device

Don't reuse old password

Indonesia

Two-Factor Authentication

THE RISE OF PANDAVA

ADAPTED FROM THE GREAT WAR OF KURUKSHETRA IN MAHABHARATA STORY

The war between the good and evil lasts forever. Nevertheless in Mayapada, the realm of human kind in the epic of Mahabharata, the Kaurava managed to have Pandava cornered.

I'm on my way..

Unable to withstand the onslaught of Kaurava cyber-attacks, Ghatotkach - the Pandava warlord, immediately dashed into Khayangan asking for God's guidance to overcome Kaurava's cyber-attacks.

O God... Our password protection somehow failed to protect us from Kaurava's cyber-attacks

My Lord, teach me how to master that knowledge.

Brave knight, son of Bhima, bear in your mind that the reign of password is over now!

Kaurava's supercomputer can easily crack passwords within seconds.

But there is ONE THING that CAN STOP THEM from doing it.

Ghatotkach came to see Batara Guru, the God of Wisdom.

All Pandava troops must start protecting their devices and accounts with "TWO FACTOR AUTHENTICATION"

WHY 2FA?

1. HACKERS MUST GET ANOTHER FACTOR OF AUTHENTICATION TO GET INTO THE ACCOUNT.

2. EVEN IF THE PASSWORD AND USERNAME ARE LEAKED, AS LONG AS THE OTHER PARTY DOES NOT HAVE ANOTHER AUTHENTICATION FACTOR, THEY WILL STILL NOT BE ABLE TO ACCESS THE ACCOUNT.

3. IF SUDDENLY YOU RECEIVE AN OTP CODE WHILE YOU ARE NOT ACCESSING ANY ACCOUNT, IT CAN CONCLUDED THAT THERE HAS BEEN AN UNAUTHORIZED ATTEMPT TO ACCESS THE ACCOUNT.

Japan

Patch Your Psychological Security Hole

Patch Your Psychological Security Hole

Resistance to Social Engineering

Starting with searching trash cans, this method has been used for all kinds of fraud, including money transfer fraud such as "leading a person into a situation where they cannot make rational decisions", methods of controlling the other party's behavior to extract necessary information, or in many cases where important information is stolen because of believing that "no one is watching" or "no one would be looking without permission" or letting your guard down. Company information and personal information are important assets. To protect your assets, be wary of "vulnerabilities of the mind"!

What Is a "Social Engineering" ?

This is a method of stealing vital information such as passwords that are needed to break into networks. Many of these methods take advantage of the psychological vulnerabilities of humans and behavioral mistakes.

XXX company entrance

I wonder if there are any data DVDs or important documents here.

Business trash

"Trashing"

Going through garbage cans, a technique that does not require direct contact with a target.

Use a shredder, etc. to ensure that documents or DVDs data cannot be restored!

This is director XYZ!! I want to get into the building but the lockcode is changed! Nobody told me! Tell me the code, right now!

Make sure to confirm the identity of the person on the other end of the phone!

Hello, this is Abcd !!

"Name Dropping" "Hurry Up"

"Name Dropping" (Eliciting information by appearing to have authority), and "Hurry Up" (To get information by rushing a target) to control the situation where the target cannot think normally, elicit the necessary information or have the target perform a requested action.

Classic Social Engineering

For scams in general, including bank transfer scams, calling it "a commonly-used social engineering technique that targets psychological security holes" gives you an idea of its nature.

Social Engineering in the digitalized generation

Social Engineering in the digitalized generation also uses manipulation in the same way.

"Shoulder Hacking"

For example, as a way to obtain valuable information without direct contact with the target, the PIN code or pattern lock of someone using their smartphone on the train can be stolen using "Shoulder Hacking" while standing behind them.

Someone may be peeking over your shoulder!

Lock code is 1126...

The pattern lock is Z-shaped

Never leave your smartphone or tablet unattended even for a short time!

"Looking at Finger Traces on the screen"

Or the pattern lock of a smartphone left on a table can be discovered by picking it up and looking at the finger traces on the screen. By identifying how to unlock the smartphone in advance, you can obtain all of their other personal data by stealing their smartphone later.
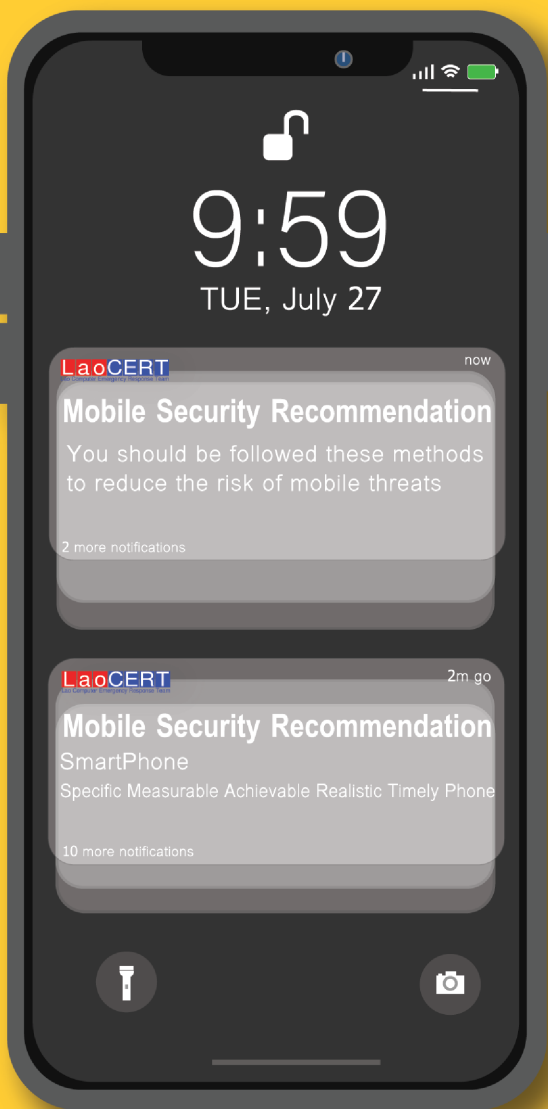
Lao PDR

Mobile
Security
Recommendation

Mobile Security Recommendation

You should be followed these methods to reduce the risk of mobile threats

Use a strong password to lock the screen

Check privacy and security, Especially turn on finding my phone

Keep your phone software updated

Don't save essential information on mobile phone

Be careful when connecting to free Wi-Fi, Especially do not process any financial

Be careful before click links

Don't forget to log out from the application when you are not used

99% of mobile threats occurred from a lack of understanding of how to use mobile safety, so awareness-raising is the most essential.

LaoCERT 9:59 TUE, July 27

LaoCERT
Mobile Security Recommendation
You should be followed these methods to reduce the risk of mobile threats
2 more notifications

LaoCERT 2m go
Mobile Security Recommendation
SmartPhone
Specific Measurable Achievable Realistic Timely Phone
10 more notifications

Malaysia

Online Presence Security

Online Presence Security

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY
MALAYSIA

What is online presence?

Online presence is **any existence** of an individual, organization or business that can be found via an online search or the **internet**

To protect our **privacy**

To protect from **cyber criminals**

To safeguard our **personal** and **confidential information**

Why we need online presence security?

Data Leakage

Identity Theft

Cyberbullying

Hacking

Malware

Pishing

Ransomware

Online Scam

What are the dangers during online presence?

How can we protect our online presence?

Do not share personal information online

Use strong and unique password for every login

Turn-off 'Save Password' feature in web browser

Use Two-Factor authentication

Make online purchase from secure site

Avoid using public wi-fi

Install and update an antivirus in every device

Perform routine Back-up

Myanmar

Ransomware
in Mobile Device

RANSOMWARE IN MOBILE DEVICE

Android 5%
iOS 3%
Mac OS 7%
Window 85%
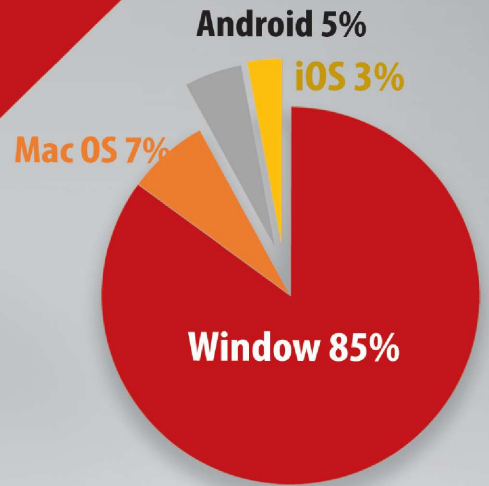
Source: purplesec.us

TYPES OF MOBILE RANSOMWARE

▸ Lock-screen types

▸ File-encrypting type

INFECTION VECTORS

- Social Network Links/ Embedded Hyperlinks
- Malicious and Fake Mobile Apps
- Compromised/ Infected Websites
- Phishing Email, Email Attachments
- Drive-by Infections
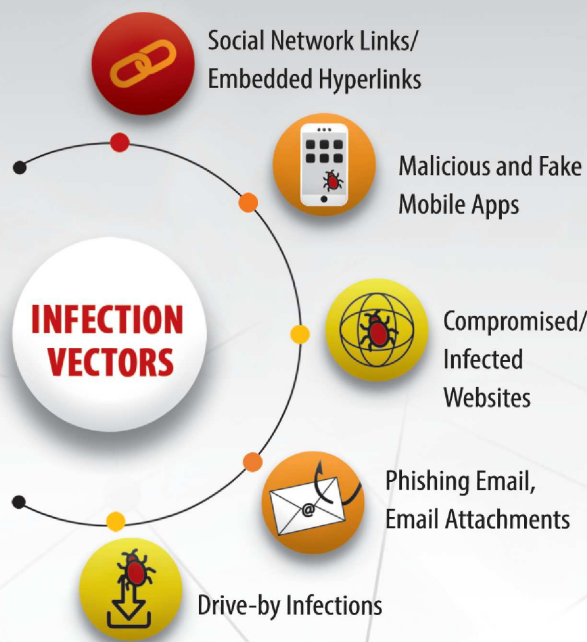
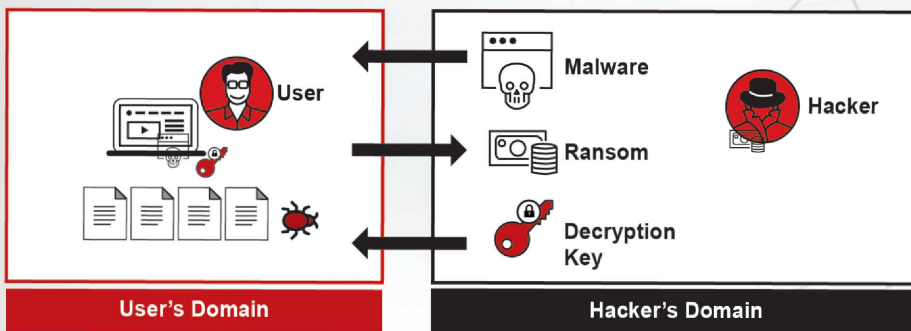## Damage costs predicted to reach
20 Billion USD by 2021

Source: cybersecurityventures

RISKS OF INFECTION

▸ Destroy Backups
▸ Steal Credentials
▸ Leak Stolen Data
▸ Publicly expose Victims
▸ Threaten victim's customers

PROCESS OF RANSOMWARE

User

Malware

Ransom

Decryption Key

Hacker

User's Domain

Hacker's Domain

Expected to attack a business
Every 11 SECONDS by the end of 2021

Source: cybersecurityventures

WAYS TO PROTECT RANSOMWARE

▸ Be aware of installing fake apps
▸ Back up all files
▸ Use a trusted and robust mobile security solution
▸ Keep up-to-date about the latest threats
▸ Install Security Patches

mmCERT
MYANMAR COMPUTER EMERGENCY RESPONSE TEAM

Philippines

Online Classroom Platforms

Safe Use of Online Classroom Platforms

- Set your online class to "private"

- Teachers should have a class list to ensure that students in the room are accounted for

- Don't share the class link or Meeting ID number on social media or any messaging apps

- Enable password for each session

- Don't let anyone use your account for your online classes

- Teachers should appoint a co-host that could take control of the class in case he/she gets kicked out of the room

- Regularly update application

- Avoid using third party apps like video and voice recording, during class

@CYBERSECgovph

DICT CYBERSECURITY BUREAU

Singapore

Email Extortion Scam

WHAT IS AN **EMAIL EXTORTION SCAM**?

What should you do if you receive an extortion email?

Learn how this scam works and what you should do to avoid falling victim.

HOW THE SCAM WORKS

1 You receive an email claiming that your device/account has been compromised

2 Scammer claims to have your 'private and confidential' information

3 A ransom is demanded to keep the information private, typically in a currency called Bitcoin

4 Scammer may use your email and password from past data breaches as 'proof' that the email is legitimate

WHAT SHOULD YOU DO?

Do not make payment. Delete the email immediately.
To prevent unauthorised access, you should:

Set strong passwords that are long and random

Do not use personal information (e.g. NRIC) in your passwords

Use different passwords for different accounts

Enable Two-Factor Authentication (2FA) when available

Your One-Time Password (OTP) is 557325

Perform anti-virus scans on all devices

Auto Updates ON

Keep your software up-to-date

WANT TO LEARN MORE? Visit www.csa.gov.sg

Thailand

How to Use
Mobile Safely

HOW TO USE MOBILE SAFELY

LOSING MOBILE MIGHT BE MORE DANGEROUS THAN YOU COULD IMAGINE

PERSONAL DATA OR ORGANIZATIONS' CLASSIFICATION DATA MIGHT BE **LEAKED AND RANSOMED**

THE POSSIBILITY IN BEING **DIGITALLY TRACKED AND FRAUD** COULD EMERGE

IMPORTANT DATA MIGHT BE **STOLEN** AND CANNOT BE **RETRIEVED**

BETTER SAFE THAN SORRY

☑ **BE AWARE OF THE DATA** AND APPLICATIONS **YOU HAVE ON YOUR MOBILE**

☑ APPLY **"DOUBLE LOCK"** BY USING MOBILE PASSCODE FOR MOBILE ACCESS AND USE PASSWORD FOR APPLICATION LOG IN

☑ DO NOT FORGET TO **LOGOUT** FROM APPLICATIONS WHEN THEY ARE NOT USED

☑ **DO NOT SAVE** ANY **PASSWORDS** IN YOUR MOBILE

☑ **ANDROID** TURN ON **FIND MY DEVICE**
iOS TURN ON **FIND MY iPHONE**
THE APPLICATIONS THAT CAN BE LOGGED IN FROM BROWSERS TO LOCK OR RESET YOUR LOST PHONE

WHEN THE DAMAGE IS DONE

☑ NOTIFY THE APPLICATION SERVICE PROVIDERS SUCH AS e-BANKING SERVICES FOR **SUSPENSION**

☑ **CHANGE PASSWORDS** FOR EVERY APPLICATION IN YOUR PHONE

☑ **NOTIFY THE POLICE** TO TRACK CRIMINAL ACTIVITIES AND TO KEEP THE NOTIFICATION AS EVIDENCE IN CASE CRIMINAL ACTIVITIES ARE COMMITTED VIA YOUR PHONE

☑ ACCESS FIND MY DEVICE OR FIND MY iPHONE TO **LIMIT THE ACCESS AND DELETE THE IMPORTANT DATA REMOTELY**

Vietnam

Free Apps

FREE APPS -
COSTLY EXPERIENCE

Remove untrusted apps which can
exploit sensitive information from your smartphone

ASEAN · JAPAN
Cybersecurity Cooperation