Computer Hygiene

The increased reliance on using computer/laptop for work and study has become critical because a lot of sensitive data is stored on these devices. This puts us at risk to cyber threats such as data leak, hacking devices, phishing attacks, etc.

Immediate action required!

- Create a strong and unique password that contains at least 12 characters along with numbers, symbols, upper and lowercase letters.
- Use two-factor authentication (2FA).
- Install full disk encryption software such as VeraCrypt/BitLocker, FileVault or use an encrypted USB for protecting sensitive data.
- Encrypt your email and messages.
- Setting up anti-virus software. E.g. Malwarebytes, Microsoft Windows Defender, Avast.

Long term security tips

- Use a password manager to help you remember your passwords. E.g. KeePassXC.
- Keep your computer operating system and software updated.
- Download and use official apps/software from the official store.
- Ensure your firewall is enabled and up to date.
- Lock your device when you're away.
- Back up files regularly on a local external disk.
- Be cautious of public WiFi.
- Protect your connection to the internet by using a VPN. E.g. ProtonVPN, Tunnel Bear.
- Use safe and updated browser:
- For browser, use Firefox, Chrome, Chromium and add extension (E.g. HTTPS Everywhere, uBlock Origin) to make internet browsing safer.
- Change your default search engine to a privacy-minded website. E.g. DuckDuckGo.
- Be aware of phishing attack.

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia @sec_matters

Mobile Phone Hygiene

Most individuals and organisations use their smartphones to login into their emails and social media pages. This puts us at risk to mobile threats such as data leak, network spoofing, ransomware, phishing attacks, etc.

How to reduce the risk of mobile threats?

- Encrypt your mobile phone by setting up a passcode in the privacy setting.
- Lock your mobile with a strong password/PIN/passcode.
- Do not save any passwords and essential information on your mobile.
- Back up all files on your mobile to an external storage.
- Location settings and mobile phone tower triangulation.
- Be aware of the data and applications you have on your mobile. E.g fake apps.
- When downloading apps, be aware of those that ask for unnecessary permissions.
- Logout from applications when they are not used.
- Checking permission of each application.
- Setting up anti-virus software/app.
- Keep your phone operating system and software updated.
- For iOs, turn on "Find my iPhone"; for Android, turn on "Find my device". These applications can be logged in from the browser to lock or reset your lost phone.
- Do not use public WiFi to process any financial or essential matters.
- Be aware before you click any links.
- Clearing your mobile of all apps and browsing history before donating, selling, or trading them in.

What to do when the damage is done?

- Notify the application service providers such as e-banking services for suspension.
- Change passwords for every application in your mobile.
- Notify the police to track criminal activities in case they are committed via your mobile.
- Access "Find my device" or "Find my iPhone" to limit the access and delete the important data remotely.

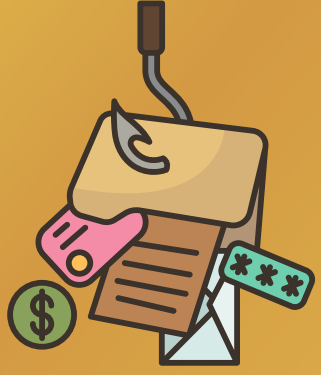
SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

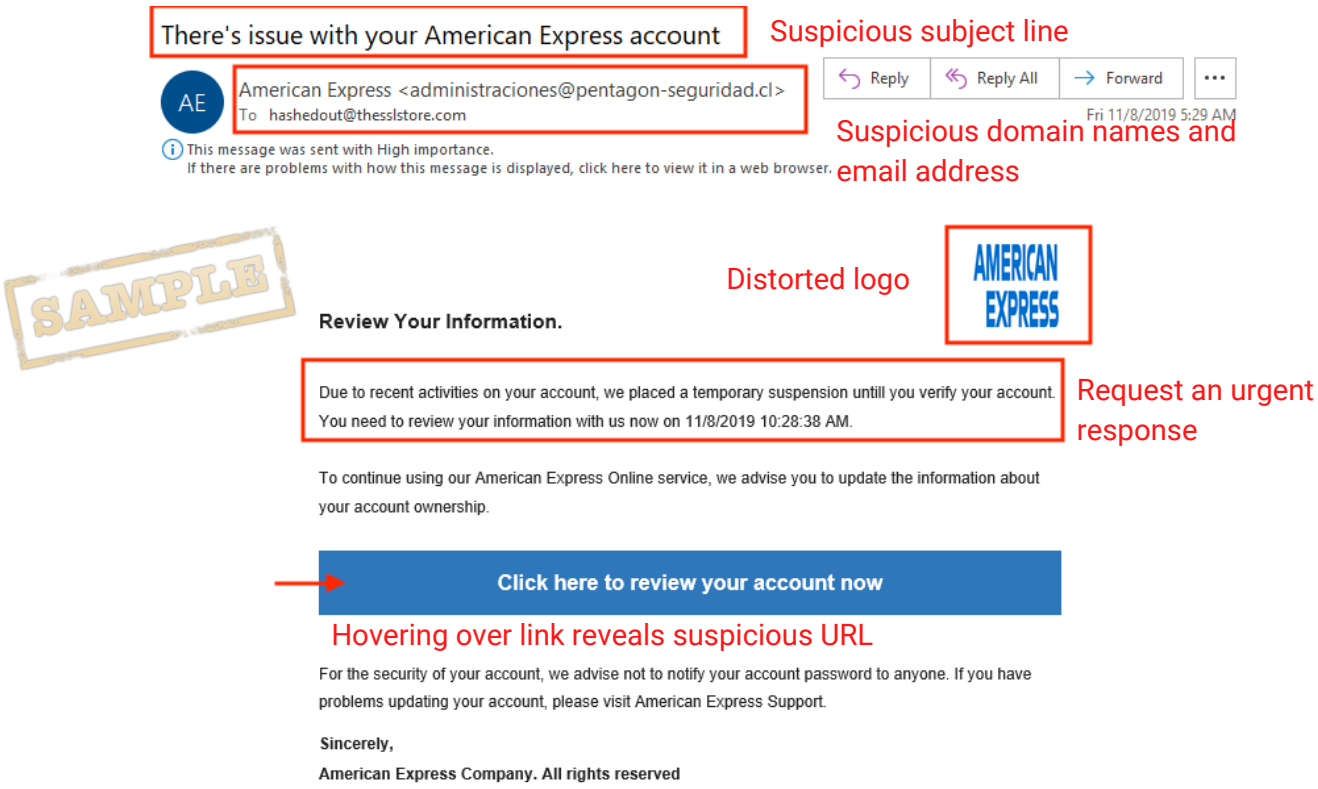
More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia @sec_matters

Phishing Attack

Phishing is a form of cybercrime in which the scammer asks you to provide them with your personal information through email, telephone, or text message by pretending to be someone else. Common phishing ploys are government imposter scams, fake person scams, love scams, and employment scams.



How to identify phishing email and message?



What should you do?

- Always check the spelling of the sender's email address, domain names, and any URL links in the email.
- Watch out for URL redirects, where you're sent to a different website with an identical design.
- Do not post personal information publicly on social media.
- If you receive an email from a source you know but it seems suspicious, always check with them first.
- Pay attention to poor spelling and grammar.
- Do not download any unknown attachments.
- Be aware of emails that sound too good to be true.
- Run a search at https://ccid.rmp.gov.my/semakmule/. Only applicable in Malaysia.
- Always think before you click!

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia @sec_matters

Online Account Security

Always strengthen your account password and enable two-factor authentication (2FA) to avoid phishing attacks, identity theft, and account hacking!

Password Management

- Create strong and unique password which containing at least 12 characters along with numbers, symbols, upper and lowercase letters.
- Use password manager to help you remember your passwords. E.g KeePassXC
- Lock your device with strong password/PIN/passcode.
- Use separate password for each account and app.
- Do not reuse old password.
- Do not share your password to others.
- Change your password regularly.
- Enable two-factor authentication.

Examples of Two-Factor Authentication (2FA)

Password + Email verification OR SMS verification OR Authenticator Apps (E.g. Authy, Google Authenticator)

How to enable 2FA on your social media account?

WhatsApp
Settings > Account > Two-factor Verification

Instagram
Settings > Security > Two-factor authentication

Telegram
Settings > Privacy & security > Two-step verification

LinkedIn
Settings > Sign in & security > Two-step verificaton

Facebook
Settings & privacy > Settings > Security and login > Use two-factor authentication

Twitter
Settings & privacy > Account > Security > Two-factor authentication

Apple
Settings > [Your Apple ID] > Password & security > Turn on two-factor authentication

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

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia @sec_matters

Secure Communication

Instant Messaging App

What makes a messaging app secure?

- All messages are encrypted end-to-end by default.
- Open-source code.
- “Disappearing messages” feature that allows you to make both received and sent messages automatically disappear after a set amount of time.
- Nearly no users’ metadata collection. Most texting apps have started adopting end-to-end encryption. However, some of them are still gathering users’ metadata.
- Allow password lock.

How to secure your communication?

Signal

- We would recommend Signal for a secure instant messaging app as it fulfill all the security features as mentioned above.
- To verify your conversation is encrypted: Open one's chat > Tap the name of the contact > Verify safety number > Scan the QR code on each other’s screens or compare the digit numbers > Tap "Mark as Verified" (iOS) or the "Verified" toggle (Android) when the codes match up.

Telegram

- Set up two-step verification.
- Start your conversation with ‘Secret Chats‘ (activate manually) that will protect your conversations with end-to-end encryption. *Regular conversations are not encrypted.
- Set up “disappearing message” on Secret Chats that you wish to disappear automatically after a set amount of time. Select a conversation > Click the three dots at the top right > Set self-destruct timer
- Lock your conversations with passcode lock.
- Terminating active sessions on other devices. Settings > Privacy and security > Active sessions > Terminate session

WhatsApp

- Set up two-step verification.
- To verify your conversation is encrypted: Open one's chat > Tap the name of the contact > Encryption > Scan the QR code on each other’s screens or compare the 60-digit number. A green check mark will pop up onscreen if the code is the same for your contact. (Conversation encrypted)
- Set up “disappearing message” for the selected conversation that you wish to disappear automatically after a set amount of time. Select a conversation > Click the three dots at the top right > Info > Turn on disappearing messages
- Turn off last seen status. Settings > Account > Privacy > Last seen > Select Nobody
- Disable auto group addition. Settings > Account > Privacy > Groups > Select My Contact or Nobody.
- Avoid auto back up your files/photos in the cloud.
- Deactivate your WhatsApp when your phone gets lost.

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

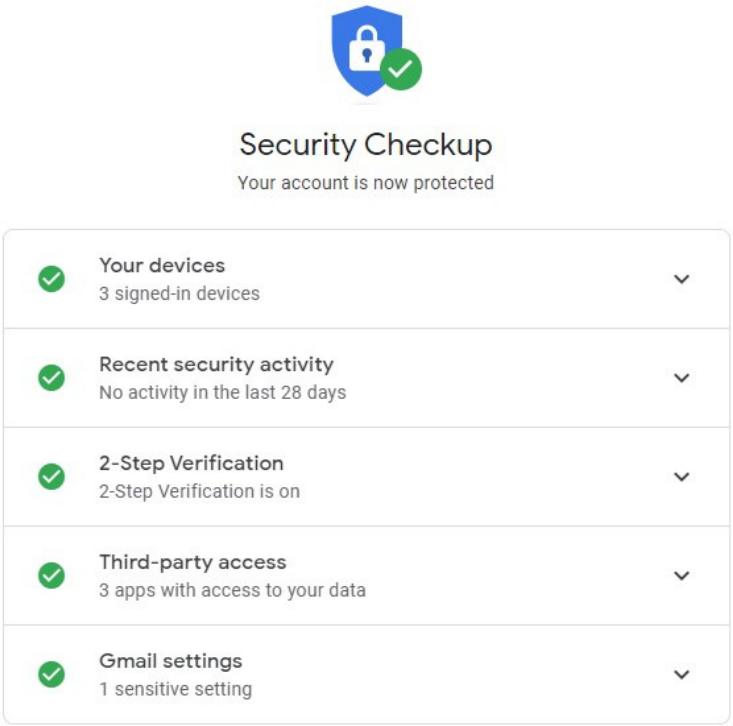
More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia @sec_matters

Secure Communication

Email Communication

- We would recommend **Thunderbird, Protonmail, or Tutanota** for secure email communication as the emails are end-to-end encrypted, the platforms are open source and support PGP encryption.
- However, since most of us are using Google and Gmail, here's how to make your Google services safer.

1. **Set up two-factor authentication.** Avoid using "Voice or text message" as it is the least secure of the available options.
2. **Check what devices have used your account.**
3. **Check recent activity** on your account under "Recent security activity" and active devices using the account under "Your devices".
4. Go through Google's Security Check-up (https://myaccount.google.com/security-checkup) for a step-by-step review of every item Google's system identifies as a potential security issue.



General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia @sec_matters