SECURITY MATTERS
NEWSLETTER

# BEWARE OF SCAMS
# SAFEGUARD YOUR ONLINE ACCOUNTS

VOL 1 • JUNE 2022

## What happened?

From the recent claims on the personal data of millions of Malaysians being sold online, personal data of employees under vaccination programmes leaked, and various online scams to bank accounts being hacked, trends of cyber attacks are increasing in Malaysia and Thailand as threat actors are continuously adapting their techniques to target and infiltrate IT environments.

The phishing scam is still a popular attack vector as humans continue to be vulnerable, careless, and naïve. Scammers will usually contact you by email, phone call, or text message and trick you into revealing your personal information. Some also use malicious software that masquerades as legitimate apps, such as banking apps, in order to trick you into downloading them, collecting sensitive information, and breaking into your account.

## How to reduce the risk of threats?

- Create strong and unique password and change your password regularly. Use separate password for each account and app.
- Install anti-virus and anti-malware software.
  E.g. Malwarebytes
- Only download official apps from the official stores.
  E.g. Apple App Store, Google Play
- Do not download Android Package (APK) files/app from illegitimate sources. The safety of your phone SMS system must always be protected as it will receive an OTP (one-time password) from various applications installed on mobile phones.
- Be aware when giving out any confidential information over the Internet/phone or any other channels.
- Monitor your accounts and activity for any suspicious activity.
- Set up two-factor authentication (2FA) on your instant messaging app, email, and social media account.
  E.g. Google Authenticator, Authy
- Keep your operating system and software updated.
- Be aware of phishing attacks especially fishy online links/attachments that trick you to click and see it. Do not reply to the message. If you might have responded to an SMS, email or phone scam, contact your bank/related party immediately.
- Do not share your ATM card number, PIN number, username, password and Transaction Authorisation Code (TAC) number. Do not respond to requests to update 3rd party TAC mobile number.
- Do not access any sensitive information through public Wi-Fi, such as logging into your bank or checking sensitive work emails. If you have to, use a Virtual Private Network (VPN) instead.

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

SECURITY MATTERS
NEWSLETTER

# BEWARE OF SCAMS
# SAFEGUARD YOUR ONLINE ACCOUNTS

VOL 1 • JUNE 2022

## How to set up two-factor authentication (2FA)?

2FA requires two ways of proving your identity and also used to protect your various online accounts.

**WhatsApp**
Settings > Account > Two-factor Verification

**Instagram**
Settings > Security > Two-factor authentication

**Telegram**
Settings > Privacy & security > Two-step verification

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

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

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

**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

**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

SECURITY MATTERS
NEWSLETTER

# BEWARE OF SCAMS
# SAFEGUARD YOUR ONLINE ACCOUNTS

VOL 1 • JUNE 2022

## How to check App permissions in my mobile device?

**Apple**
Settings > Privacy > Tracking > Allow Apps to request to track

**SAMSUNG**
Settings > App > Install unknown Apps

**HUAWEI**
Settings > Security > More settings > Install Apps from external

**xiaomi**
Settings > System & device > Additional settings > Privacy > Unknown sources

**realme**
Settings > Security > Unknown source installations

**OPPO**
Settings > Password & security > System security > Installation sources

**vivo**
Settings > Apps & permissions > Permission management > Install unknown Apps

Always consider what an app does before accepting any permissions. Some apps require permissions that are completely unnecessary to their primary function.
E.g. Youtube downloader app, request permission to send SMS to you (suspicious)

**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