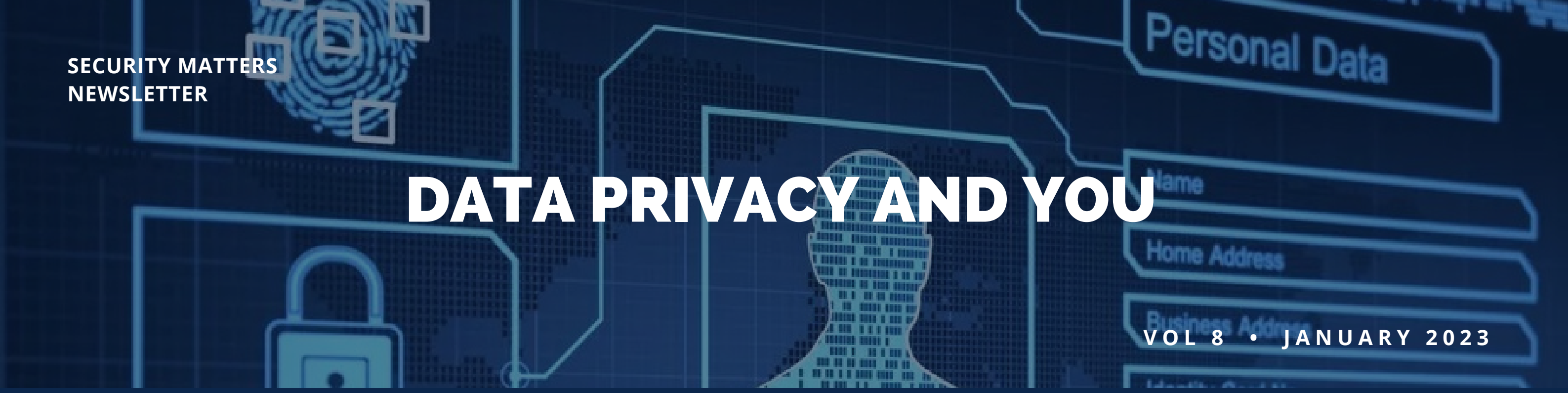
SECURITY MATTERS
NEWSLETTER



DATA PRIVACY AND YOU

VOL 8 • JANUARY 2023

Our digital lives are more active, whether it's our everyday data for online banking, eCommerce, social media or business-level security around regulations. Everyone is a target. No matter if you're an individual or running a business. We exposed a lots of personal identifiable information (PII) online. These data can be used to learn things about you, your habits, interests, and can be monetized or used by malicious actors to steal your identity or hack your accounts.

Some of the common PII:

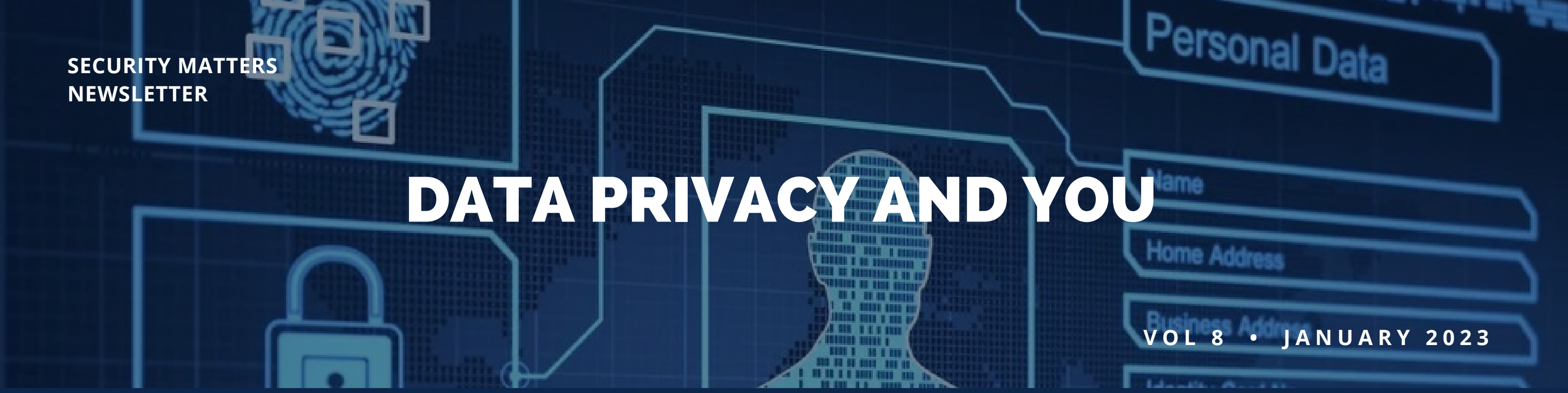
- Full name
- Credit/debit card number
- Email address
- National ID number
- Phone number
- Date of birth
- Passport number
- Biometrics (Face, fingerprint, etc)
- Home address
- Birth place
- Genetic info

Many users are unaware about how their personal information is being used, collected, or shared online. Some examples of privacy concerns include social media sites that sell access to users through individualized advertising that puts them at risk and many medical apps including exercise trackers and calorie counters do not have the best security. And even though we know about these, what are we doing to protect ourselves and our organizations? When was the last time you reviewed data privacy best practices with your team members? Let's start to be aware of the risks and take steps to protect our personal information.

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

More information about Security Matters, visit www.securitymatters.asia
✉ info@securitymatters.asia
@secm8
@sec_matters

SECURITY MATTERS
NEWSLETTER



DATA PRIVACY AND YOU

VOL 8 • JANUARY 2023

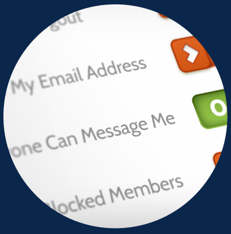
Here are some valuable tips that you can use to protect your personal information

Password security

- Set up strong and unique passwords/passphrase. E.g. Th3bus1n3ss1sg00D! (the business is good!).
- Do not reuse passwords.
- Do not use same password for multiple accounts.
- Do not use the ‘Remember me’/'Save my password' functionality especially for online banking.
- Use a password manager. E.g. KeePassXC
- Enable two-factor/multi-factor authentication (2FA/MFA)

Data Encryption

- Turn on encryption on all devices. Make sure your devices have complex passwords or passcodes or PINs.
- On Apple devices, turn on FileVault.
- On Android, make sure encryption is turned on in the “encryption and credentials”.

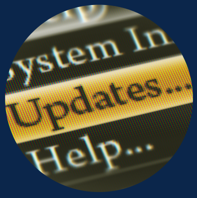


Configure Privacy Settings & Check Privacy Policy

- Customize advanced device privacy and browser settings. Block auto cookie and location tracking. Disable auto-download and auto-run of Flash.
- Check your privacy settings on social media. Know what you are sharing on social media.
- Check the privacy policy before you download any apps.

Bluetooth & WiFi Settings

- Change the default password and username for WiFi network to a unique one.
- Avoid using public WiFi networks. Use a Virtual Private Network (VPN) if you really need to.
- Disable Bluetooth and WiFi when not in use.

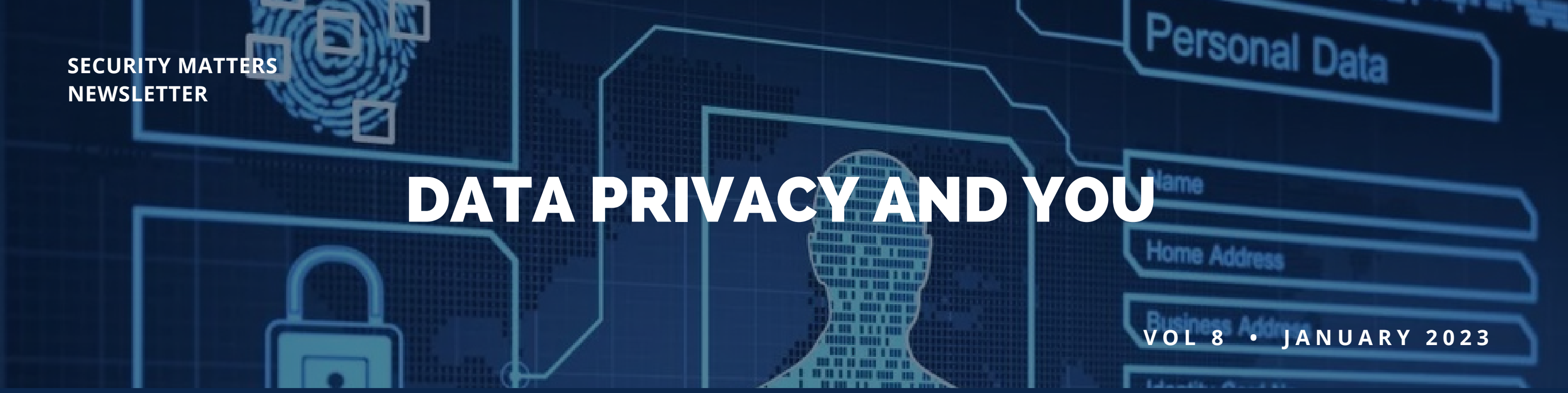


Updates Software

- Keep your software and apps updated.
- Always use anti-virus and anti-malware software. E.g. Malwarebytes

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

More information about Security Matters, visit www.securitymatters.asia
✉ info@securitymatters.asia
@secm8 @sec_matters



SECURITY MATTERS
NEWSLETTER

DATA PRIVACY AND YOU

VOL 8 • JANUARY 2023

Data Sharing & Permission

- Be aware of what apps you use. Always check the "Apps permission", does the app really need to access your location/contact lists? Delete any apps that you don’t use anymore.
- Try turning off as many data sharing options off as you can, and only turn on if you really need them.
- Be cautious of what you share online.
- Be aware of the apps and websites you use and the information they request.
- Do not send sensitive data in an email.

Avoid Unknown Sites & Links

- Be careful of suspicious emails, phone calls, or text messages.
- Verify the source before clicking on any links/attachments or enter personal information in response to unsolicited messages.
- Only use trusted sites for your online shopping, and only provide personal information or credentials over secure links (check if the site address begins with https://)

Secure Cloud Services

- Adopt a secure cloud service to eliminate the risk of sharing files through USBs or unsecured emails.

Monitor Access & Report

- Keep a close eye on your financial accounts, including credit card and bank statements. Monitor for any suspicious activity and report it immediately.
- Check if any of your accounts were implicated in known data breaches.

Taking steps to protect your personal data from cybercriminals is essential. By following the steps above, you’ll be able to frustrate hackers and guarantee your own digital security. We hope that these tips helped!

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
@secm8 @sec_matters

Related News

Here's how to clear your browser cache for a clean slate in 2023

Your browser cache helps you store website data so those pages can load faster the next time you visit them. However, they might no longer match the data the sites actually need to load, and pages would actually load slower as a consequence. Here's how to clear your cache that will give those sites a fresh start in your browser and free up some space in your storage.
Read more: https://bit.ly/3QeuBbV

Data breach: How to check if your personal details are compromised and what to do to stay safe

There have been several reported news stories recently regarding alleged leaked databases, affecting the personal details of Malaysians. The breaches affected companies like TM involving 250,000 Unifi Mobile customers, Carousell affecting 2.6 million users, AirAsia allegedly leaked due to ransomware, and Maybank's recent case.
Read more: https://bit.ly/3WHeZjJ

WhatsApp launches proxy service for users to get around internet shutdowns

Users can now connect to the app using a proxy server run by a network of volunteers and organisations when it is not possible to connect directly to WhatsApp. This feature works on both iOS and Android and can be found in the app's Storage and Data settings.
Read more: https://bit.ly/3Grx12v

Meta's new ad policy further protects teen privacy and tackles discrimination

Teens will be able to – sort of – control what ads they see as Meta is updating the way it delivers advertisements to users in order to foster a more positive experience. The changes can be divided into two parts: one will restrict how companies that target teenage users while the other aims to make things more "equitable" and less discriminatory.
Read more: https://bit.ly/3CFqbVW

Men are more hit by identity thefts than women

While the entire world is speaking about gender equality in every work-field, we observe things to be going contrarily in the world of cyber security. According to a research, Men are twice as likely to be targeted by Identity Theft attacks as Women, as the latter seem to be more cautious while making their personal information online.
Read more: https://bit.ly/3W6hdI2

Latest phishing campaign hits Zoom users with malware

Hackers usually target communication tools like Zoom to easily deliver malware to the user's machine. This IcedID malware was used in a phishing campaign. This malware primarily targets businesses and can be used to steal payment information. it usually spreads via spam emails with malicious Office file attachments.
Read more: https://bit.ly/3k6EqfY

Credential stealing flaw in Google Chrome impacted 2.5 billion user

The vulnerability that impacted over 2.5 billion Google Chrome users and all Chromium-based browsers, including Opera and Edge. It allowed remote attackers to steal sensitive user data like cloud service provider credentials and crypto wallet details.
Read more: http://bit.ly/3XdtLPh

Call to action: Recycle your old phones

More people are likely to keep old mobile phones than recycle them, preventing precious minerals from being harvested. MCMC first introduced its mobile ewaste initiative in 2015, with the goal of educating the public about safely disposing of unwanted or unused devices that have reached their end-of-life.
Read more: http://bit.ly/3ZDbqg8

How to properly delete all your personal data before selling your smartphone

If you ever want to sell your smartphone to someone else, make sure you erase all traces of personal data before it gets into the wrong hands. A few simple steps can help you protect your data before you part ways with your handset.
Read more: http://bit.ly/3wDGz5G

12 Ways to improve your website security

In today's digital age, a business website is essential for success. To ensure that your site is effective and safe, you need to make sure that it has all the necessary security features. Check out more ways here.
Read more: http://bit.ly/3HaMB2A

<Threat Analysis and Protection Mechanism of Human Rights Defenders in Malaysia, Thailand and Indonesia>
Read report here:
https://bit.ly/3BTW8cu

THREAT ANALYSIS AND PROTECTION MECHANISMS OF HUMAN RIGHTS DEFENDERS IN MALAYSIA, THAILAND, AND INDONESIA

PREPARED BY SECURITY MATTERS 2021/2022

SECURITY MATTERS
www.securitymatters.asia

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
@secm8 @sec_matters