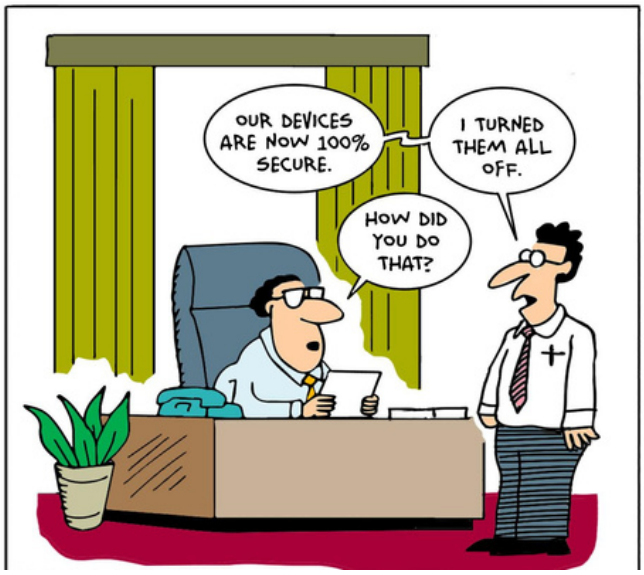
Security Matters

NEWSLETTER



BEST PRACTICES TO SAFEGUARD YOUR MOBILE DEVICES

Mobile devices have become an intrinsic part of everyday life. People are no longer just using them for texting, social networking, and entertainment. How private and secure is your smartphone? How easily could someone read your sensitive information if your mobile device is lost or stolen? How well do app developers and internet service providers protect that data? And what can you do to protect yourself? Many mobile users are running devices with known vulnerabilities. Many still didn't take minimal security measures like using a screen lock, backing up data, or installing an app to locate a missing phone or remotely erase data from it.

Mobile security refers to the protection of mobile devices such as smartphones, tablets, wearables, and other portable devices from hacking and other dangers that could steal data or harm the device. Why is it important to protect your mobile devices? Because they store a large amount of personal and sensitive information and are frequently used to access financial services, making them prime targets for cybercriminals. Most individuals and organisations use their smartphones and laptops to log into their emails, social media pages, and online transactions. This puts us at risk as we are increasing our digital footprints on our mobile devices day by day.

COMMON SECURITY THREATS TO MOBILE DEVICES

Data Breach/Leakage

Mobile devices are small, portable, and easy to lose or to be stolen. It often has access to sensitive data. If these devices are compromised due to malware, phishing, or physical theft, this data can be exposed. Such breaches can lead to financial and productivity losses.

Unauthorized Device and Data Access

Access to the device and its contents may be gained by forging or guessing the authentication PIN or password or by bypassing the authentication mechanism entirely.

Malicious Apps and Links

Hackers upload malicious programs or games to third-party smartphone application marketplaces, the programs steal personal information and open backdoor communication channels to install additional applications and cause other problems. Malicious links on social networks are also a way to spread malware where hackers can place Trojans, spyware and backdoors.

Malware and Spyware

Mobile malware and spyware come in the form of Trojans, adware, ransomware, and viruses. Malware can be spread through internet downloads, messaging services, and Bluetooth communications. Once infected with your device, the malware mines private data and sends it to third parties. Hackers use spyware to hack phones, allowing them to hear calls, see text messages and emails as well as track someone's location through GPS updates.

Phishing Attacks

Anyone can trick you into giving access to your accounts or providing your personal information by sending you fake links or emails. When you open an email, check the email address of the sender. Be careful downloading attachment files or clicking links. Any links that ask you to take action, be aware of the urgency, threats, or requests for help.

Excessive App Permission

App permissions determine an app's functionality and access to a user's device and features, such as its microphone and camera. Some apps are riskier than others. Some can be compromised, and sensitive data can be funneled through to untrustworthy third parties

Unsecured Wi-Fi Networks

Mobile devices transport data via wireless networks, which are typically less secure than wired networks. Do not access any sensitive information through public Wi-Fi, such as logging into your bank or checking sensitive work emails, as a hacker may be able to intercept your communication through a "man-in-the-middle" attack.

Network Spoofing

Hackers set up fake access point connections that look like Wi-Fi networks, but that are trapped in high-traffic public locations such as cafes, libraries, and airports. In some cases, attackers require users to create an "account" to access these free services, complete with a password. Hackers can compromise user's email, e-commerce, and other secure information. And whenever you are asked to create a login, whether for Wi-Fi or any application, always create a strong and unique password.

Outdated Devices

Devices that are too old to receive security updates should be replaced. Even if it seems to still be running, there's a risk in using an old device that hasn't received the latest security updates.

" WHEN IT COMES DOWN TO IT, JIM, SECURITY IS A PERSONAL RESPONSIBILITY."

BEST PRACTICES TO SAFEGUARD YOUR MOBILE DEVICES

Screen Lock

- It can be set up with a pattern, fingerprint, PIN, password, or facial recognition.
- For iPhone users: try using a **6-digit PIN password** instead of the default 4-digit PIN, or using an **alphanumerical password**. Avoid simple/repeating numbers like “123456”, “1111111” or “password”. Create a password with min 15 characters, containing upper and lower case letters, numbers, and special characters.
- For Android users: use a **PIN** or **alphanumerical password** rather than the lock screen pattern design.

Download Apps only from the Official Store

- Only download apps from the official app store, e.g. **Google Play** or the **Apple App Store**.
- Check the authority of the app, ratings, and reviews if they are available.
- Read the app’s **privacy policy** and review the **app's permissions** before downloading and installing it.

Update Operating System, Software and Apps Regularly

- Security updates address security vulnerabilities that could be exploited by cybercriminals.
- It provides new features and improved performance.
- For Apple users: How to update your iPhone/iPad?
- For Android users: How to update your Android phone?

Be Cautious of Public Wi-Fi & Public USB Ports

- Always use a **virtual private network (VPN)** when connecting to public Wi-Fi. E.g. Proton VPN, TunelBear, Express VPN, Tor Guard.
- Avoid logging in to any accounts that contain sensitive information like banking or email when connected to an unsecured wireless network. If you have to, use your cellular data.
- Avoid using USB ports in public places, as they may be unsafe and can potentially install malware on your device. If you have to, use a **USB data blocker** instead.

Think Before You Click

- To avoid falling for a **phishing** scam, always check the spelling of the URLs in email links before you click or enter sensitive information.
- Always verify who is contacting you for your personal information.
- **Do not** click on any unknown attachments files or links.

Location Access & Bluetooth

- Giving location access to all apps can be dangerous as it can reveal your whereabouts to people you don't want to share it with.
- Allowing all apps to access Bluetooth can be risky as it can enable unauthorized devices to connect to your phone and access your data. The same applies to Apple's AirDrop.
- **Limiting location and Bluetooth access** can help protect your privacy and prevent unauthorized access to your data. Check how to do it below:
  How to check App permission on my mobile device?
  How to turn off location tracking?

Back Up Data Regularly

- Backing up important files and data offline, on a local external disk, or in a secure end-to-end encrypted cloud storage.
- For Apple users: **How to back up your iPhone/iPad?**
- For Android users: **How to back your files?**

Deactivate and Wipe Lost or Compromised Devices

- If your device is lost or stolen, disabling service, locking it, or completely erasing its contents remotely are the options to take.
- Devices like iPhone and Android can lock a device or erase its contents remotely through a built-in mechanism.
- If you are using Microsoft Exchange on your mobile phone learn how to perform a remote wipe on a mobile phone here.

Maintain Physical Control of the Device

- Treat it similarly to our identity card/credit card by maintaining control at all times and storing it securely if left unattended.
- If possible, avoid keeping sensitive information on a mobile device. If the presence of sensitive data is not avoidable, encrypt the data. Some devices support built-in encryption capabilities.

Always practice the habit of Digital Security Hygiene!

The more you depend on your phone for everyday tasks, the more it will impact you if your device is compromised. Therefore, protecting your mobile devices is crucial and it doesn't have to be difficult. It can be one of the simplest things you can do, by reading all of the above and practicing good mobile device security habits.

Related News

R00TKT halts its cyberattack campaign against Malaysia

International hacker group R00TK1T has put a halt on its cyberattack campaign against Malaysia's digital infrastructure, according to an announcement that was posted on its Telegram channel. R00TK1T claimed that it had successfully hacked its way into digital infrastructure that belonged to several Malaysian organisations such as the Ministry of Education (MoE).
Read more: https://bit.ly/45aF9iW

Hackers exploit job boards, stealing millions of resume and personal data

Employment agencies and retail companies chiefly located in the Asia-Pacific (APAC) region have been targeted by a previously undocumented threat actor known as ResumeLooters since early 2023 with the goal of stealing sensitive data.
Read more: https://bit.ly/47BjGB8

Pegasus spyware targeted iPhones of journalists and activists in Jordan

The iPhones belonging to nearly three dozen journalists, activists, human rights lawyers, and civil society members in Jordan have been targeted with NSO Group's Pegasus spyware, according to joint findings from Access Now and the Citizen Lab. Nine of the 35 individuals have been publicly confirmed as targeted, out of whom six had their devices compromised with the mercenary surveillanceware tool.
Read more: https://bit.ly/3wr7cOr

Scammers steal US$25 million during conference call using deepfake technology

Deepfake technology has reached a point where it's not just applicable to still images and videos like conference calls. Such was the case one unfortunate employee who got duped into handing over US$25 million (~RM119 million) to people she thought were her real colleagues during the "con" call.
Read more: https://bit.ly/3Q6CJge

Google and Yahoo have changed their policy, here's what you need to know and what to do

Google and Yahoo have introduced new policies aimed at controlling spam and enhancing email security and overall experience. They will explore the ins and outs of these policy changes, uncover why they were implemented, analyze how they affect email senders across the board, and provide some practical advice on how to adjust to the shifting email environment.
Read more: https://bit.ly/3HZme0n

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

This new Android feature could help save you from phishing and malware

Google is rolling out a new feature called Android Safe Browsing on Android phones, which is designed to alert you to harmful links and websites within supported apps. This notification will tell you about the risks before letting you open the link, so you can decide if the link is legitimate.
Read more: https://bit.ly/4bCCfqQ

Hackers gained access to TNB Electron and TNBX EV charges

The international hacker group R00TK1T has resumed its cyberattack on Malaysia just one day after putting a halt to the campaign. Since then, the group has hit several targets with among latest one being the GO TO-U (GTU) EV charging platform that TNB's subsidiary, TNBX, uses.
Read more: https://bit.ly/48lucMe

This new malware can literally steal your face to use in fraud- Android and iOS devices both affected

Chinese hackers are stealing biometric data to create deepfakes. Cybersecurity researchers have discovered a new mobile trojan that literally looks to steal people's faces (biometric data) and uses it to generate convincing deepfakes which can then be used to break into mobile banking applications. It is targeting people in the Asia-Pacific region, with those in Thailand and Vietnam being most at risk.
Read more: https://bit.ly/48lihhA

Opensignal: Malaysia lags behind Thailand and Indonesia for telco reliability

Based on Opensignal's metrics, reliability is the extent to which users stay consistently connected to their mobile network and whether they can continue to do typical tasks like email, watching videos, and using navigation apps while still connected. Malaysia is currently lagging behind its peers Singapore, Thailand and Indonesia for telco reliability.
Read more: https://bit.ly/3SPrlFG

New code of ethics for journalists to combat fake news

The journalism ethics manual has been reviewed in 35 years since it was developed in 1989 by the Malaysian Press Institute (MPI). Communications Minister Fahmi Fadzil said the newly-launched manual outlines eight fundamental ethics that underscore the responsibilities and standards expected of journalists in the country.
Read more: https://bit.ly/3Pe0YZ9

Keep your phone number private with Signal usernames

Signal is making your phone number on Signal more private. Once these features roll out, your phone number will no longer be visible in Signal to anyone running the latest version of Signal who doesn't already have it saved in their phone's contacts.
Read more: https://bit.ly/49k4n0d

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