SECURITY MATTERS
NEWSLETTER

WATCH OUT FOR THESE WHILE TRAVELLING!

VOL 2 • JULY 2022

After more than a year of pandemic lockdowns, many countries are now open its border for travelling. Numbers of international travelers has increased, be it travel for work or vacation. Being outside of their normal technology routines, travelers face a slew of increased cybersecurity threats. The vulnerabilities ranges from unsecured public WiFi networks, leaving a devices on public transport, falling victim to a fake charging station or using unprotected equipment like hotel computer/printer.

If you ever think that security is someone else's job, watch out for the risks/threats around! Security should never reside with one person as their sole responsibility, it's everyone's responsibility! Physical security is often a first step to protect your digital information. Here are some tips for keeping your devices and data secure while you're travelling.

Before you go..

Update your device software.
E.g. Operating system, anti-virus/anti-malware software, apps, etc.

Set up "Find My Device" or "Find iPhone" on your device.

Back up your information.

Minimize the sensitive data contained on the device.

Encrypt your devices and set up a strong PIN code/passcode/password on your device.

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

WATCH OUT FOR THESE WHILE TRAVELLING!

VOL 2 • JULY 2022

While you're travelling..

Stop auto connecting to wireless and Bluetooth networks.

Use a personal WiFi hotspot from your mobile phone. Connect to VPN immediately if you have to join the public network.

Avoid using public WiFi especially in the airport, hotel, train/bus station or cafe. Do not access sensitive information when accessing to public WiFi.

- Do not leave your mobile devices unattended including USB or external storage device. Keep the devices with you all the times.
- Do not connect untrusted devices to your laptop or mobile device. E.g. Free USB drive.

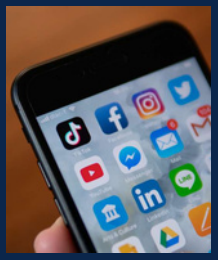
Do not store your mobile devices in checked luggage and in the car.

Lock your screen when you step away from your devices.

Avoid using shared equipment such as hotel computer or printer.

Be aware of what others can see on your screen. Dim your screen or use privacy filter.

Use USB data blockers or AC adapters when charging devices in public.



Do not post location or agenda on social media. Post only after your trip.

Shred your paper documents such as boading pass, hotel receipts, etc when you don't need it anymore.

Whether you are traveling for work or vacation, practice these tips. Stay safe and secure, have a gerat travelling experience!

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

WATCH OUT FOR THESE WHILE TRAVELLING!

VOL 2 • JULY 2022

How to remotely wiping your files/data on your device?

If your mobile device is lost, confiscated or stolen, you may be able to remote wipe the files but you will need to set up your device beforehand to do this. Note that remote wiping relies on your device being connected to the internet. Use the following guides to set up remote wipe:

Apple/iCloud

1st step: Visit www.icloud.com/find > Find My iPhone > All Devices > Select and erase Device
2nd step: Enter Apple ID password > (if you're not using a trusted browser, answer security question/enter verification code)

- If device is online, remote erase begin after follow all the instructions
- If device is offline, remote erase begin the next time it's online

See more: https://apple.co/3o6SYet

Android

1st step: Settings > Personal > Google > Services > Security > Android Device Manager > Switch On "Remotely Locate This Device" & "Allow Remote Lock and Erase"
2nd step: Settings > Switch On Location
3rd step: Visit www.Android.com/devicemanager > Sign in Google account > Find your lost/stolen device > Select the exact location of device > Wipe your Android Remotely

See more: https://bit.ly/3Pwi1DT

Microsoft

Sign in to MIcrosoft Endpoint Manager admin center > Select devices > All devices > Select the device that you want to wipe

See more: https://bit.ly/3OePOzQ

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

Japanese man loses USB drive with data on the entire city's residents

The unnamed worker lost a USB flash drive containing the personal details of every resident of the city of Amagasaki, northwest of Osaka, after going for drinks this week, according to a statement Thursday from the city's government. Public broadcaster NHK reported that the worker in his 40s, fell asleep on the street after drinking alcohol at a restaurant. When he woke up, his bag containing the flash drive was gone.
Read more: https://bbc.in/3RA1RdQ

Facebook scam: Crooks Using Messenger Chatbots to Steal Login Data

The new phishing scam uses malicious and fake chatbots to steal login credentials of unsuspected Facebook users through Facebook Messenger. These chatbots are generally used by businesses that offer live chat or customer support services.
Read more: https://bit.ly/3yMeTwb

Apple's new 'Lockdown Mode' fights hacking and targeted spyware

Apple plans to release a new feature called “Lockdown Mode” that aims to add a new layer of protection for human rights advocates, political dissidents and other targets of sophisticated hacking attacks. This feature is designed to activate "extreme" protections to its phones, such as blocking attachments and link previews in messages, potentially hackable web browsing technologies, and incoming FaceTime calls from unknown numbers.
Read more: https://apple.co/3OkmPdL

Human error blamed for leak of 1 billion records of Chinese citizens

A prominent Chinese tech CEO has cited human error as the likely reason hackers got their hands on the personal data of 1 billion people in China from a Shanghai police database and then put some of it up for sale on illicit online markets. Since people overseeing sensitive data still can’t seem to be trusted to protect it, the incident once again demonstrates that companies need to take numerous steps beyond password-protecting systems that store data to ensure that it doesn’t fall into the wrong hands, noted a security professional.
Read more: https://bit.ly/3yNS37t

Ongoing phishing campaign can hack you even when you’re protected with Multi-factor Authenticaton (MPA)

Microsoft detailed an ongoing large-scale phishing campaign that can hijack user accounts when they're protected with multi-factor authentication measures designed to prevent such takeovers. The threat actors behind the operation, who have targeted 10,000 organizations since September, have used their covert access to victim email accounts to trick employees into sending the hackers money.
Read more: https://bit.ly/3ob7PV2

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