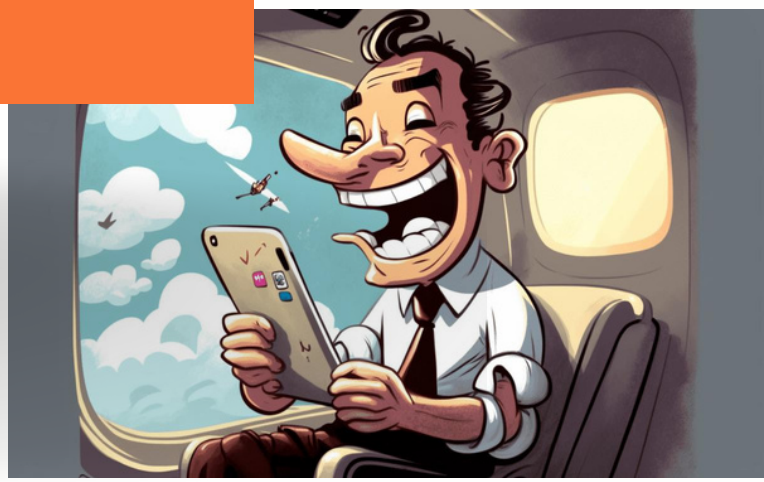
Security Matters
NEWSLETTER



GOING ON VACATION? THESE WILL HELP YOU TRAVEL SAFELY

The holiday season is here! As much as it's about fun and adventure, it's equally important to consider digital and physical security when you're on the go, especially if you're considering travel and work at the same time. Travellers often rely on technology to enhance the vacation experience, like by sharing photos online or finding lodging on an App. Just because you're travelling, it doesn't mean you should put yourself at risk of cybercrime or theft. From safeguarding personal information to your phone being tracked, below are some tips that you can do to improve your digital and physical security on the go.

Before you go

- **Update software and applications** on all devices, including operating systems and security updates.
- **Install antivirus and antimalware software** on all your devices.
- **Back up all important files/data** to a secure cloud storage service or an external hard drive. E.g. Tresorit or NextCloud.
- **Setup strong passwords or passcode or PINs** on all devices to prevent unauthorized access.
- **Encrypt sensitive data on devices** to protect against data breaches in case of loss or theft. Use device encryption tools like VeraCrypt, BitLocker, FileVault.
- **Enable two-factor authentication (2FA)** on all online accounts like social media, messaging apps, cloud storage, Google, etc.
- **Beware of scams** when you make online bookings on accommodation, especially on Airbnb. Always do research and look for reliable platforms before making online payments.
- **Travel lightly.** Limit the number of devices you take with you on your trip. The more digital devices you take with you, the more risk you open yourself up to.
- **Save emergency contacts.** Know the local emergency numbers, your telco provider number and the location of the nearest embassy or consulate.
- **Keep a copy of important documents** like passport, identity card, insurance, flight itinerary, in case of loss of theft.

On the go

Digital security

- **Disable auto-connect** to wireless and Bluetooth networks.
- **Avoid using public WiFi,** especially in the airport, hotel, train/bus station or cafe. Use a personal WiFi hotspot from your mobile phone instead. Do not access sensitive information when accessing to public WiFi.
- **Use a Virtual Private Network (VPN)** if you have to join the public network.
- **Avoid public charging stations.** Always bring your personal USB cords, and plug your charger directly into an electrical socket. **Use USB data blockers or AC adapters** when charging devices in public.
- **Turn off location services** when not in use, and consider limiting how you share your location on social media.
- **Enable tracking apps** and erasing features on devices to locate or delete data in case of loss or theft.
  [iOS] Find My iPhone **[Android]** Find My Device
- **Do not connect untrusted devices** to your laptop or mobile device. E.g. Free USB drive.
- **Beware of phishing attacks.** Avoid suspicious links, emails and calls. Always verify the source before giving out any information.
- Always ensure you're browsing on the site beginning with **"HTTPS".** HTTPS will protect you against many forms of surveillance, as well as account hijacking and some forms of censorship.
- **Be careful with social media sharing.** Do not post location or agenda on social media. Post only after your trip.

Physical security

- **Do not leave your mobile devices unattended** including USB or external storage devices. **Lock your screen** when you step away from your devices.
- Beware of your surroundings. **Beware of what others can see on your screen.** Dim your screen or use a privacy filter.
- **Avoid using shared equipment** such as hotel computers or printers. If you've been forced to use a public computer for any reason, remember to remove any trace of yourself before you log off.
- **Keep your devices with you or in your hotel room safe at all times**. Don't take out your devices in unsecured public spaces unless you need to.
- **Consider using a cheap/second-hand device** to keep stored in a secure location.

In case of loss or theft

- **Enable remote tracking and wiping for your device.** This allows you to erase your data if your device is lost or stolen.

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

- **Notify Your Bank and Mobile Carrier.** If your phone or credit/debit cards are lost or stolen, inform your bank and mobile carrier immediately to prevent unauthorized transactions.
- Keep a record of your device information. Contact the local emergency or relevant agency numbers that you've saved.

Happy Travelling!

Related News

How to know if someone is stealing my Wifi?

While wireless networks facilitate seamless internet connectivity for all of your devices, they also make it simpler for other users to access your connection. If you notice that your WiFi has been running slow for some days and you suspect that someone is stealing your WiFi, the first and foremost thing you should do is check.
Read more: https://bit.ly/45aF9iW

WhatsApp bew privacy feature let users hide location during calls

WhatsApp has begun to roll out the 'Protect IP Address in Calls' feature, which conceals your IP address during calls. Upon using this feature, all your calls will be relayed through WhatsApp's servers, protecting your IP address and preventing other callers from figuring out your geographical location.
Read more: https://bit.ly/47BjGB8

Signal now lets you to delete all trace of a contact from the app

Signal user can now decide for themselves who they want to see in the messenger's contact list and they can delete contacts from the app if no longer want them to appear there. Deleted contacts not only disappear from your Signal contact list, they are also no longer displayed when searching for contacts, and they no longer have access to your current profile photo or stories.
Read more: https://bit.ly/3Q6CJge

Scammers are hijacking Google forms and using a fake AI chatbot to steal money

Scammers have found another way to abuse a legitimate cloud service to deliver spam and phishing messages to people's inboxes. The attackers also deploy a fake AI chatbot in an attempt to steal people's cryptocurrency.
Read more: https://bit.ly/3RHSAmp

2FA Your secret weapon for digital defense

Two-factor authentication (2FA) is one such measure that has emerged as a secret weapon for digital defense, significantly enhancing the security of our online accounts. Now, we will explore the world of 2FA, its significance, and how it works to protect our digital assets.
Read more: https://bit.ly/47BjGB8

DDoS attacks are increasing in APAC

The rise in DDoS attacks correlates with Russian companies increasingly moving into the APAC region. Recently, ChatGPT became one of the biggest victims of DDoS attacks when it suffered from a periodic outage. Reports showed that the outage was due to DDoS attacks targeting its API and ChatGPT services.
Read more: https://bit.ly/3Q6CJge

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

It might not be quite awful to use Google Drive on your smartphone any more

The cloud storage platform is getting a new look homepage that sports a refreshed appearance and layout Google says will, "help you more easily find the right file much faster. What's more, the changes are being introduced across both Android and iOS, meaning users across the business (and personal) world will get a much smoother experience when accessing Google Drive when travelling or simply being away from their desks.
Read more: https://bit.ly/3RHSAmp

Google Chrome officially starts clamping down on third-parry cookies

After the initial testing period, the company will begin its phased rollout of the cookie replacement program from Q3 2024. The deprecation of third-party cookies is designed to reduce cross-site tracking, but it will also present challenges to “sign-in, fraud protection, advertising, and generally the ability to embed rich, third-party content in websites.
Read more: https://bit.ly/45aF9iW

How multi-stage phishing attacks exploit QRs, CAPTCHAs and Steganography

Phishing attacks are steadily becoming more sophisticated, with cybercriminals investing in new ways of deceiving victims into revealing sensitive information or installing malicious software. One of the latest trends in phishing is the use of QR codes, CAPTCHAs, and steganography. See how they are carried out and learn to detect them.
Read more: https://bit.ly/3RHSAmp

Hackers abusing WhatsApp messages to install Android malware

Microsoft recently uncovered a series of mobile banking trojan campaigns meticulously designed to exploit unsuspecting users in India. This expose delves into the sophisticated strategies employed by cybercriminals utilizing social media platforms like WhatsApp and Telegram to manipulate users into installing malicious apps, posing as reputable entities ranging from banks to government services.
Read more: https://bit.ly/3RHSAmp

Microsoft's Windows Hello Fingerprint authentication easily bypassed by cybersecurity firm

If you’re using a premium or even a basic-yet-decent Windows laptop, chances are you’ll have a fingerprint sensor on it. This fingerprint sensor is also typically one of the easiest way for you to sign into your laptop which on the surface promises a biometric form of security ensuring only you or anyone with your finger can access your laptop.
Read more: https://bit.ly/3RHSAmp