SECURITY MATTERS
NEWSLETTER

BE CAREFUL OF YOUR FOOTPRINTS WE KNOW ABOUT YOU..

VOL 12 • MAY 2023

Information is king in the digital age, and consumer data is a valuable resource. Every time you do something online, be it banking, shopping or commenting on social media posts, you leave a digital footprint, essentially a trace of yourself in cyberspace, just like your physical footprints. Your digital footprint can be used to learn more about you and gain your trust. These data can be read by your employers, friends, family, strangers, and cybercriminals. It can be used by marketing companies to send targeted advertisements, or worse, used by cybercriminals to commit identity theft. The more information you put online, the more people can learn about you.

ACTIVE footprints

Intentionally made on the internet such as,

- Email address
- Text messages
- Phone number
- Signing up forms
- Creating an online account
- Making purchases online
- Comments on articles or posts
- Photos or videos on social media sites.

PASSIVE footprints

Made without your intention of doing so. You do not realize that someone collects information about your activity. Examples,

- Cookies and tracking data created by your web browsing activity
- Geolocation data when using maps
- Other apps that can track your location & IP address

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

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

SECURITY MATTERS
NEWSLETTER

BE CAREFUL OF YOUR FOOTPRINTS WE KNOW ABOUT YOU..

VOL 12 • MAY 2023

How to remove your digital footprints?

Unfortunately, it's not possible to remove your digital footprints entirely. There will always be some information that you cannot erase that is held by third parties and hidden from you. However, you can remove a lot of this data by following the tips below:

Unsubscribe
We are sorry to see you go!
Confirm
Are you sure you want to delete your account?
No
Yes

Delete posts, pictures or videos you no longer want to be associated with.

Delete unnecessary information you do not want the website or service stored on their end such as home address, phone number, date of birth, etc.

Unsubscribe from mailing lists that you don't really read or need.

Remove accounts that you are not using anymore.

Remove any data stored on your device, browsing history, cookies and cache.

Review and update the privacy settings for all your online accounts. Limit the amount of data that is collected and shared.

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

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

SECURITY MATTERS
NEWSLETTER

BE CAREFUL OF YOUR FOOTPRINTS
WE KNOW ABOUT YOU..

VOL 12 • MAY 2023

How to protect your digital footprints?

Search your name online and know what's out there about you.
Check for compromised credentials by using tools like "Have I Been Pwned?"

Protect your devices by setting up PIN numbers and two-factor authentication (2FA).

Protect your main email address. Use a different email for a throw-away account. Separate work and personal accounts.

Review your app permission. Deny any apps if you don't feel they're necessary.

Use digital tools to manage your digital footprints by using incognito mode (private mode) in Mozilla Firefox and Google Chrome.

Log out of all apps and sites you've previously used.

Learn how to spot phishing, social engineering, and other common online scams.

Avoid oversharing on any social media websites or on public forums. Always think before you post/share!

Create strong passwords and set up 2FA on all of your accounts. Use a password manager (e.g. KeePass XC) to manage all of your passwords.

Avoid public Wi-Fi. Use a Virtual Private Network (VPN) if you have to. This is to hide your browsing habits.

Disable location tracking. Delete cookies and cache regularly to clear tracking data.

Use a privacy-focus tool like DuckDuckGo instead of Google as your default search engine.

Install browser extensions that block ads and trackers. E.g. uBlock Origin, Privacy Badger, HTTPS Everywhere, NoScript.

Use the "Checkout as a Guest" option for online shopping.

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit www.securitymatters.asia

info@securitymatters.asia
@secm8
@sec_matters

Related News

Several telcos to block sending SMS with URL links

Several telecommunication companies in Malaysia will be blocking the ability to send or receive URLs through the short message service (SMS). This block will include SMS that ask for personal particulars such as a person's name as well as their identity card number, bank account or other contact details.
Read more: http://bit.ly/43k0zto

Vietnamese threat actor infects 500,000 devices using 'Malverposting' tactics

A Vietnamese threat actor has been attributed as behind a "malverposting" campaign on social media platforms to infect over 500,000 devices worldwide. Malverposting refers to the use of promoted social media posts on services like Facebook and Twitter to mass propagate malicious software and other security threats.
Read more: https://bit.ly/40TSNnK

Google blocked over 1.4 million malicious apps from Google Play Store

Google has brought in many verification methods for Android app developers like Phone, email, and other verification methods, which will prevent malicious developers from deploying their apps in Google Play Store.
Read more: https://bit.ly/40XEbnk

How to spot a ChatGPT phishing website

Hackers will always take advantage of the hot thing: COVID-19, crypto, tax season, or what have you. And with the rise of ChatGPT, they've not missed a beat. They are leveraging the popularity of ChatGPT in phishing attacks.
Read more: https://bit.ly/3LPsWb8

Before you download an App, watch out for these red flags

Mobile apps can be incredibly useful, but they also come with risks. Some apps may pose a threat to your privacy and security, so it’s important to be cautious before downloading them. Read more for the red flags here.
Read more: https://bit.ly/419pSMB

Singapore woman who scanned QR code with malware lost S$20,000 to a survey scam

She visited a bubble tea shop and saw a sticker pasted on its glass door, encouraging customers to do an online survey to get a free cup of milk tea. She scanned the QR code on the sticker and downloaded a third-party app onto her Android phone to complete the “survey”. Scammers used the app she had downloaded to take over her device and moved S$20,000 (RM66,000) from her bank account.
Read more: https://bit.ly/3HQVHmh

Vietnam to require social media users to verify identity

Vietnam is preparing to make it mandatory for social media users of both local and foreign platforms to verify their identity in a bid to rein in online scams. The measure to be issued by the end of this year, will enable law enforcement agencies to track down offenders using social media to break the law, state-run Voice of Vietnam (VOV) newspaper reported.
Read more: https://bit.ly/42yzmlw

Deepfake scams exposed

Cybercriminals are now using deepfake video technology to make fraudulent calls and appropriate money. According to Kaspersky, AI can gather data on your physical movements and human face. Deepfake technology has created video technology products with sound and images that fake real-life objects with high accuracy.
Read more: http://bit.ly/3JgNaJm

Truecaller will soon be able to identify spam calls over WhatsApp

Caller identification app Truecaller has revealed that it is working on integrating its service into WhatsApp and other messaging apps. This will help WhatsApp users identify spam callers when receiving voice calls through those apps just like how Truecaller works with regular calls.
Read more: https://bit.ly/3B9mQ02

WhatsApp introduces chat lock for better privacy

WhatsApp is introducing a new privacy feature - Chat Lock, which lets you hide any chat behind, as you might guess from the name, a locked folder. This extra layer of security lets you lock up certain chats that are hidden from your inbox and can only be accessed by either your device password or biometrics, such as fingerprints and face scans.
Read more: https://bit.ly/3n9pL5x

Google will start deleting inactive accounts after two years

Google has announced an update to its policies that includes changes to how it will handle inactive accounts. As of now, accounts that have been inactive for over 24 months (two years) may have the contents across services such as Gmail, Drive, Photos, Docs, Sheets, Slides, Drawings, Forms, and Jamboard deleted. This also applies if your account has gone over the storage limit for over two years.
Read more: https://bit.ly/3n9pL5x

Don't click that ZIP file! Phishers weaponizing .zip domains to trick victims

A new phishing technique called "file archiver in the browser" can be leveraged to "emulate" a file archiver software in a web browser when a victim visits a .ZIP domain. With this phishing attack, you simulate a file archiver software (e.g., WinRAR) in the browser and use a .zip domain to make it appear more legitimate.
Read more: https://bit.ly/3n9pL5x

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

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