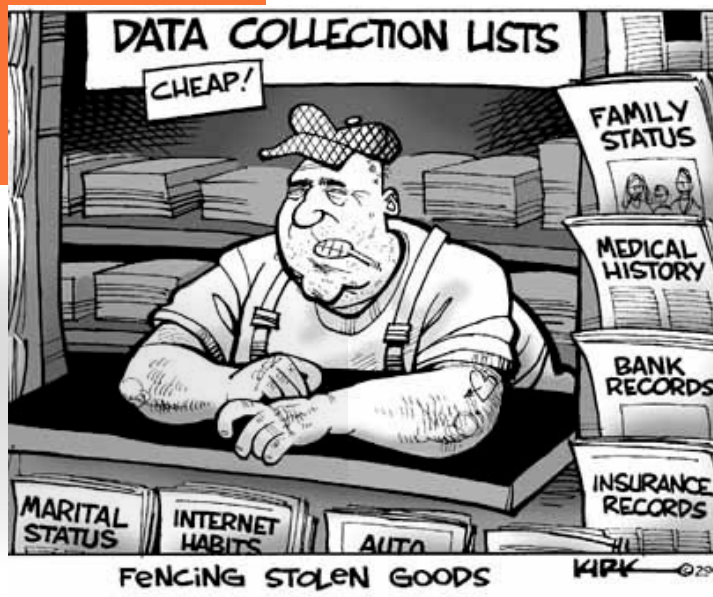
Security Matters

NEWSLETTER



UNVEILING THE MYTHS OF DATA AND ONLINE PRIVACY

Today, data privacy is becoming more important and challenging with Artificial Intelligence (AI) becoming a game-changer in the industry. As the digital landscape evolves, it is imperative for businesses and individuals, and even for those in the realms of journalism and activism to fortify their digital defences.

In general, data privacy relates to the protection of personal information or data from unauthorized access, where your personal information is collected, processed, stored or shared regardless of the online or offline medium. Online privacy specifically focuses on the protection of personal information shared and collected through digital channels, especially on the internet, such as browsing websites and social media, online transactions, etc.

There are many myths and misconceptions surrounding this topic that can lead to confusion and vulnerability. Let's embark on a journey to unveil the truth about data and online privacy, enabling you to understand more about the digital realms and take steps to protect your personal information.

#1 Strong passwords are enough to protect my data.

Truth: While strong, unique passwords are crucial, they are just one layer of security and it is insufficient. Phishing and hacks can both compromise passwords.

What to do: Implementing two-factor authentication (2FA), keeping software updated, use a password manager, and using encrypted connections to protect your data.

#2 Encryption is the only solutions to secure data.

Truth: While encryption is important, it's just one tool in the data privacy toolbox. Numerous measures and procedures can be implemented to keep data secure.

What to do: Other measures like restricting access to sensitive data, enable 2FA, implementing data governance policies, backing up data, regular security audits, keeping the software and security measures updated, etc.

#3 I have nothing to hide. So I don't need to worry about data privacy.

Truth: Privacy is not just about hiding information, it's about protecting your personal space and autonomy. Even if you believe you have nothing to hide, your digital activities, if exposed, can be misused, leading to identity theft, financial fraud, or even reputational damage.

#4 I'm not a famous person, I'm just a regular citizen, nobody cares what I do online.

Truth: Everything you do on the internet matters. The search terms you use, the web pages you visit, and the choices you make all play a role in what you are being exposed to online.

#5 Data breaches only happen to other people, not me.

Truth: Data breaches can happen to anyone, regardless of how careful they are with their personal information. Don't assume that you're immune to data breaches

What to do: Practise digital security hygiene to protect yourself.

#6 I can't be identified if I don't share personal information.

Truth: Everyone who uses the internet can be identified through de-anonymization. In practice, you already have what's known as a digital fingerprint, or unique information about your device, system, and browser that separates you from others.

What to do: Avoid using invasive software/apps, use a private browser or VPN, and clear your browser history and cookies regularly.

#7 Once data is deleted, it's gone forever.

Truth: Deleted data may still exist on servers or backups. Cybercriminals can still retrieve your documents, images, and other files using easily accessible "recovery" tools found online. You should be mindful of what you share as complete deletion is not always guaranteed.

What to do: You can physically destroy hard drives before recycling an old computer or properly erase your hard drive, by downloading disk wipe tool like Data Shredder. For smartphones, opt for a "restore" or "factory reset".

#8 It's safe to use public Wi-Fi because everyone does it.

Truth: While Wi-Fi hotspots are free and easy to use in many places, even if it's a legitimate hotspot, there's a risk for someone nearby who's trying to access your info or hack your device.

What to do: Avoid using public Wi-Fi, use your hotspot instead, or use a trusted VPN to browse anonymously.

#9 Private browsing/Incognito mode is completely private.

Truth: Incognito is just a tool in your privacy toolkit. While they prevent your browsing history and cookies from being saved on your device, they don't cloak your online activity from everyone. Website, Internet Service Provider (ISP) and even employers can still track what you're doing online.

What to do: To enhance your privacy, use a VPN (e.g. Tunnel Bear, ProtonVPN) or secure browsers (e.g. Firefox, Tor browser), use a search engine like DuckDuckGo.

#10 Any VPN will keep my online traffic safe and private.

Truth: Not all VPNs were created equally. There are different ways to run a free VPN, and most of them involve monetizing users' data. Always remember, when a valuable service is provided for free by a for-profit company, you're not the customer, you're the product.

What to do: Recommended to use a paid VPN (e.g. Express VPN), or you can choose a free VPN like Tunnel Bear, or ProtonVPN.

#11 Data privacy is only for big companies. Small and medium-sized businesses aren't at risk of data loss.

Truth: Hackers target individuals and small businesses just as frequently as big companies. Small and medium-sized businesses are often seen as easier targets because they may lack data protection measures and security teams as big companies. Just because your company has never experienced a data attack before doesn't mean it won't happen in the future.

#12 Data protection cost a lot of money.

Truth: Protecting your data doesn't have to cost a lot of money. In many cases, it can actually save you money. There are several simple and effective steps you can take to protect your data.

What to do: Encrypt your email and messages, using a password manager, enable 2FA, use a VPN, back up your data regularly, beware of phishing attacks, keep your software updated, etc.

#13 Only the IT department is responsible for data protection

Truth: While the IT department plays a major role in an organization's data protection program, ultimately, it is everyone's responsibility to appropriately handle and protect data. The IT team is there to educate, and assist with the software and security concerns, not to do data protection for everyone.

Data is collected from you for a reason. You can either give up that data or take steps to protect it. At the end of the day, being proactive with your data privacy and security is the way to go. Protecting yourself online is your responsibility.

Check these out on how to protect your digital life.

Digital Security Fact Sheets

Data Privacy and You

Related News

Kaspersky's iShutdown tool detects Pegasus spyware on iOS devices

Kaspersky has introduced a new tool that lets users detect Pegasus, a popular iOS spyware known for targeting journalists and activists. This lightweight method called iShutdown will identify signs of spyware on Apple iOS devices, including Pegasus, QuaDream's Reign, and Intellexa's Predator. It also designed to identify other malware threats on iOS devices.
Read more: https://bit.ly/45aF9iW

[Malaysia] Omnibus Act will be enacted this year

The Omnibus Act is expected to be enacted this year to allow data sharing and cloud storage among government agencies. The implementation of data integration from every government agency needs to be supported through strong and sustainable data sharing legislation, said the Economy Ministry secretary-general.
Read more: https://bit.ly/47BjGB8

Google Incognito mode: new disclaimer reveals data tracking

Google Chrome's private browsing mode promised a cloak of anonymity, letting users roam the web free from watchful eyes. But a recent lawsuit and a quiet update by Google have cast a shadow over this digital haven, raising questions about its effectiveness and the company's commitment to user privacy.
Read more: https://bit.ly/3RHSAmp

WhatsApp on Android could soon let you share files with nearby friends

WhatsApp may receive its own version of Apple's AirDrop as a recent Android beta shows hints that a file-sharing feature is in the works. What's particularly interesting about this file sharing is the receiving person will need to physically shake their smartphone to create a share request.
Read more: https://bit.ly/3Q6CJge

AdGuard launches free temporary email generator

AdGuard, an ad-blocking service, has announced Temp Mail, its new feature that will help keep your inbox spam-free. The service is useful to create a disposable email any time you need to sign up for something like services or free trials but do not necessarily want to give out your personal email.
Read more: https://bit.ly/3RHSAmp

One of the biggest data leaks ever has just been revealed

A massive database containing the gains of thousands of data breaches has been found online, amounting to 12TB and comprising over 26 billion records, making it the largest ever discovered.
Read more: https://shorturl.at/mpqCT

Beware of pirated MacOS Apps that install Chinese malware

A new malware has been found embedded in pirated macOS applications, which downloads and executes several payloads to compromise devices in the background. Specifically, these apps are hosted on Chinese pirate websites to entice more victims.
Read more: https://bit.ly/3RHSAmp

Telekom Malaysia's entire customer database allegedly put up for sale

A database seller has claimed to have a massive database that belonged to TM. According to the data sample that the seller attached to the listing, it has the user's name, gender, address, and phone number alongside MyKad number, salary range, and marital status. The database even has the mother's name as one of the data fields which we assumed is being used for security purposes.
Read more: https://bit.ly/3RHSAmp

Why it's important to turn on Apple's new Stolen Device Protection?

Apple rolled out an update to its iOS operating system this week with a feature called Stolen Device Protection that makes it a lot harder for phone thieves to access key functions and settings. Check out more on how does it works.
Read more: https://bit.ly/3RHSAmp

iPhone apps abuse iOS push notifications to collect user data

Numerous iOS apps are using background processes triggered by push notifications to collect user data about devices, potentially allowing the creation of fingerprinting profiles used for tracking. According to mobile researcher Mysk, who discovered this practice, these apps bypass Apple's background app activity restrictions and constitute a privacy risk for iPhone users.
Read more: https://bit.ly/3RHSAmp

Using Google search to find software can be risky

Google continues to struggle with cybercriminals running malicious ads on its search platform to trick people into downloading booby-trapped copies of popular free software applications. The malicious ads, which appear above organic search results and often precede links to legitimate sources of the same software, can make searching for software on Google a dicey affair.
Read more: https://bit.ly/45aF9iW

The simplest way to defeat a phone scam, more tips to protect yourself in the AI age

Phone scams like these have been around for years but have become more targeted as people share information more freely online. And as technology like voice cloning improves, emotion-driven scams seeking to wheedle cash out of unsuspecting victims, such as the one that nearly befell a Marin County family, have only gotten more convincing.
Read more: https://bit.ly/45aF9iW

Malicious ads on Google target Chinese users with fake messaging apps

Chinese-speaking users have been targeted by malicious Google ads for restricted messaging apps like Telegram as part of an ongoing malvertising campaign. The latest iteration of the campaign also adds messaging app LINE to the list of messaging apps, redirecting users to bogus websites hosted on Google Docs or Google Sites.
Read more: https://bit.ly/3RHSAmp

Hacker group R00TK1T threatens to attack Malaysis's digital infrastructure

Prior to its newly announced threat to Malaysia, R00TK1T claimed to have attacked several high-profile targets in the past few months. Among them is the French cosmetic company, L'Oreal in which the group claimed to obtain its "inner workings" and order database.
Read more: https://bit.ly/3RHSAmp

Citizen Lab details ongoing battle against spyware vendors

Citizen Lab senior researcher Bill Marczak said that while the organization has achieved some important wins against spyware proliferation, the progress is inevitably hindered by vendors that continually adapt their technologies and practices. He emphasized that defending against the threat, which governments commonly use to target human rights activists and journalists, is increasingly challenging and requires government regulations.
Read more: https://bit.ly/45aF9iW

Microsoft 365 users need to be on their guard

A new report from Trustwave cybersecurity researchers SpiderLabs has claimed hackers are increasingly turning to the Greatness phishing kit due to its advanced features, simplicity in use, and relatively low cost. Greatness was developed by a threat actor going by the alias "fisherstell" and has been available since mid-2022, primarily targeting Microsoft 365 office software users.
Read more: https://bit.ly/3RHSAmp

How Apps exploit push notifications and ways to stop them

The comfort of push notifications keeps us notified about messages, updates, and alerts from different apps. Yet, recent disclosures have revealed a concerning factor of this technology—apps manipulating push notifications to gather user data without permission. Check out more on how apps use push notifications for intrusive tracking and how users can safeguard their privacy.
Read more: https://bit.ly/3RHSAmp

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