Security Matters

NEWSLETTER

BACK TO BASICS. DIGITAL SECURITY A TO Z

In today's threat landscape, where cyberattacks can feel like a never-ending game of hide-and-seek. Digital security is a shared responsibility, and each one of us can contribute to a safer digital environment. The only way to win the long fight against breaches, theft, and hacks is by working together, sharing knowledge, and reinforcing good digital security hygiene. Although Cybersecurity Awareness Month just passed, it's never too late to refresh on the basics and educate ourselves and others on how to stay safe online.

Let's go back to the basics A to Z. The list below is more like the **common digital security terms** that you have heard and the best practices you need to know to protect yourself against cyber threats.

A

- Always check the **App** permission list before downloading an **App.**
- Install **antivirus** and **anti-malware** software. E.g. Windows Security, Malwarebytes, Avast

B

- **Backup** your data and files regularly to an external disk or secure cloud storage.
- Choose your **browser** wisely. Recommend using Firefox as the default browser.

C

Choose your **cloud storage** wisely. Recommend using a private cloud storage. E.g. Tresorit or NextCloud. Encrypt your data/files before uploading to the cloud.

D

- Secure your **devices** with a strong PIN code or passwords
- Only **download** official apps from the official stores. E.g. Apple App Store, Google Play.

E

- **Encrypt** your devices with software like VeraCrypt, BitLocker, FileVault, or use an encrypted USB for protecting sensitive data.
- **Encrypt** your email and messages.

F

A **firewall** can restrict internet traffic from accessing your private network. Ensure your **firewall** is enabled and up to date.

G

Gateways serve as the entry and exit points for all data, converting information from one format to another. E.g. A Wi-Fi router is a gateway between computer and internet service provider's network.

H

- Always ensure you're browsing on the site beginning with "**HTTPS**".
- Check your browser settings. Clear your download and browsing **history**, cache, and cookies regularly.

I

Identity theft occurs when someone uses personally identifiable information in order to impersonate someone else. Practice digital security hygiene to protect your online privacy.

J

Beware of **job scams**. Do your research and verify its legitimacy before applying for a job. Keep your personal information safe from strangers online.

K

Keyloggers is a kind of spyware software that records every keystroke made on a computer's keyboard. It can record everything a user types including instant messages, email, usernames, and passwords.

L

Think before you click on **links** and attachments. Beware of short URL links.

M

Malware (malicious software) is designed to damage or enable unauthorized access, to computer systems. E.g. virus, worm, Trojan horse, rootkit, ransomware, spyware/adware.

N

Review your **network** router settings.
Secure your router by using a strong password.
Set up your wireless router with an encryption standard like WPA2.

O

Beware of **online scams** like government imposter scams, love scams, job scams, giveaways, debt collection, etc. Always check and verify if it's a legitimate source.

P

- Create strong and unique **passwords** and change your password regularly.
- Beware of **phishing** attacks. Learn how to spot phishing and other common online scams.

Q

Be cautious when scanning **QR codes** from unknown sources.
Use reputable and secure QR code generators.
Verify the destination before scanning a QR code to ensure its legitimacy.
Limit the use of QR codes for sensitive information.

R

Ransomware is a form of malware used to threaten victims by blocking or corrupting their data until a sum of money is paid.
Always think before you click.

S

- Be cautious of **social engineering** and phishing attacks.
- Review your **social media** privacy settings and remove any inactive accounts. Be careful what you post on social media.

T

Set up **two-factor authentication (2FA)** on your instant messaging app, email, and social media account.
E.g. Google Authenticator, Authy

U

- **Update** Operating system and software regularly.
- Use **USB** data blockers or AC adapters when charging devices in public.

V

Use a **Virtual Private Network (VPN)** to keep your online activity private.
E.g. Proton VPN, TunnelBear, Express VPN

W

Avoid using public **WiFi** to access personal information, especially in the airport, hotel, train/bus station, or cafe.

Z

A **zero-day exploit** is when hackers discover a software gap or flaw they can use to gain access to users' information or computers. Therefore, update your system and software, practice digital security hygiene regularly.

Related News

Proton unveils "World first" censorship-resistant CAPTCHA

ProtonVPN has just unveiled its very own secure CAPTCHA service. Proton CAPTCHA solves issues within existing systems that website providers use to discern between genuine login attempts and malicious bots. The tool claims to never compromise privacy, security, and accessibility, while describing itself as "the world's first" CAPTCHA with built-in censorship-resistant technologies.
Read more: https://bit.ly/3RHSAmp

Malicious HDMI cables steals photos, videos, and location data

John Bumstead, who works for a company called 404Media that fixes and sells used electronics, found an iPhone-to-HDMI adapter that seemed normal at first. However, the app that came with it was tricky because it asked users to scan a QR code. This code leads to an ad-filled website, prompting downloads of an invasive app that requests various permissions, collects data, and sends it to China.
Read more: https://bit.ly/45aF9iW

European companies sold spyware to despots: media

European companies sold powerful spyware to authoritarian regimes which have used it against dissenters. "During the last decade the Western world has encouraged and applauded the digital tools that empower democracy activism in countries under authoritarian regimes. But at the same time European companies have supplied such authoritarian regimes the digital back doors to turn any digital device into powerful spying tools against dissenters," European Investigative Collaborations (EIC) said.
Read more: https://bit.ly/47BjGB8

Beware of GoldDigger malware will drain your bank accounts without you even realizing

A dangerous new Android malware strain has been observed making the rounds, capable of stealing money from dozens of banking apps. The malware was being delivered via two separate apps - one impersonating a Vietnamese government portal, and another one impersonating an energy company.
Read more: https://bit.ly/3Q6CJge

Watch out - this nasty Android trojan can record your video and audio calls

Cybersecurity experts are warning Android users to be careful when downloading applications from third-party sources, as they could end up installing some nasty malware. SpyNote, as they found, comes with numerous information-stealing capabilities. It can access call logs, the camera, SMS messages, external storage, and can take screenshots, record video and audio.
Read more: https://bit.ly/3RHSAmp

Fake friends and followers on social media - and how to spot them

Social media has had an immeasurable effect on our lives, including on how we engage and interact with other people. Yet not everything is always as it seems on social media. As per the internet in general, these platforms have become a hotbed for scammers and fake news peddlers. One of the biggest threats to watch out for on social media is fraud perpetrated by people who aren't who they claim to be. Here's how to recognize them.
Read more: https://bit.ly/3F4EROY

Beware that Google Chrome update alert might actually just be malware

There are multiple fake "update your browser" campaigns active right now that are aiming to trick people into installing all kinds of malware on their devices. Once they gain access, they modify the site to display a popup that impersonates Google, Mozilla, Microsoft, or other companies with their own browser (depending on what the user is running at the time of the visit).
Read more: https://bit.ly/47BjGB8

Cybercriminals using online scams to profit from Israel-Gaza conflict

There has been an increased in online scams targeting donating funds to victims of the Israel-Gaza conflict. Scammers send out emails requesting aid – then scam those who respond. Users need to be extra-vigilant in identifying such scams.
Read more: https://bit.ly/47BjGB8

Hackers using secure USB drives to attack government entities

An ongoing attack on government agencies in the APAC region has been claimed to have compromised a secure USB device with hardware encryption. The nation's government agencies utilize these safe USB devices to transfer and save data between computer systems.
Read more: https://bit.ly/47BjGB8

You should update WinRAR now

If you're someone who uses WinRAR to handle your archived files such as ZIP and RAR files, you need to immediately update WinRAR when you can. This comes after a major security vulnerability in the popular trialware file archiver was found.
Read more: https://bit.ly/47BjGB8

Beware of phishing scam involving fake 'WhatsApp Web' pages

Police warned that WhatsApp Web could be a new variant of phishing scams. The links took victim to phishing websites embedded with the genuine QR code extracted from the official website of WhatsApp. When victims scanned the QR code on the phishing website with their mobile phones, the page became unresponsive and scammers gained remote access to their WhatsApp accounts.
Read more: https://bit.ly/3Q6CJge