Digital Security

Digital Security is the protection of one’s identity online. It involves and details tools and means to secure your identity and assets in the online and mobile world.
Phishing

These are fraudulent attempts to obtain sensitive information like credit card details, passwords, and usernames by disguising as a trustworthy entity in electronic communications like emails. These emails normally have poor grammar and spellings, poor email design and quality includes a false sense of urgency and directly solicits personal or financial information.
Pharming

A hacker redirects an internet user to a fake website instead of a legitimate one with an intention of capturing a victim’s sensitive information like passwords, usernames and credit card information.
A form of malware attached to internet pop-ups or downloadable files once installed, they can monitor your keystrokes, read and delete your files, reformat your hard drive and access your personal details without your knowledge.
Zoom Bombing

Unwanted intrusions into a video conference showing obscene or lewd things by an uninvited individual causing disruption. Similar situations happen with WebEx, Skype.
5 simple steps to avoid Zoom bombing

- Avoid using your personal meeting ID.
- Always use a meeting password.
- Use Zoom’s waiting rooms.
- Mute audio and disable video for meeting attendees.
- Turn off screen sharing for everyone apart from meeting’s hosts.
Tips for Online Safety

- Install an antivirus and keep it updated - An Antivirus protects your device from all kinds of malicious software.

- Use unique passwords for every time you log in - Almost all pages we visit require us to create user accounts but we can’t keep track of all these passwords, in that case, a password manager is important, some free managers include Last pass, Dashlane, and Keeper.

- Get a VPN and use it - Ensure to use a Virtual Private Network (VPN) every when you are using public WI-FI. VPNs encrypt your internet connection making it private.

- Use two-factor authentication - Two-Factor Authentication, add another layer of authentication on top of your username and password as you log into your accounts. Platforms like Facebook, Gmail and even WhatsApp have it, be sure to enable it.
Tips for Online Safety

■ Use passcodes even when they are optional. Most smartphones offer passcode options - be sure to activate them and on top of that use biometric authentications like fingerprints to ensure stronger security.

■ Clear your cache - Your browser’s cache knows a lot about you, saved searches, cookies all which could trace back to your personal data.

■ Turn off your “Save password” feature in all browsers - Browsers have an inbuilt password management system, turn that off and use password managers

■ Avoid click baits - Be smart about what you click to avoid being a victim of phishing. Look out for suspicious websites or emails typically requesting for personal information.

■ Protect your social media privacy - Limit the amount of private information you share on social media like home address, phone numbers, and bank details

Ensure to update your devices always - Regularly updating your software and operating systems helps to reduce security vulnerabilities
End-to-End encryption simply means encrypting communications to make them unavailable to third parties. Through encrypted platforms, information is transmitted using a secret code rather than an insecure plain text.

Fig. 1a: Encryption in transit

Fig. 1b: End-to-end encryption

Fig. 1c: End-to-end encryption (no service provider)
Signal offers end-to-end encryption by default on all its communications.

Whatsapp, because of encryption, WhatsApp doesn’t store your messages on its servers.

Line offers a “letter sealing” feature which enables End-to-End encryption on multiple devices.

Telegram offers more privacy options like secret chats and a timely self destruct option for photos, files, and messages.
How to De-google your life

- Search differently, use alternative search engines like DuckDuckGo.
- Consider using a different browser like Firefox and Brave.
- When using Google, try searching in incognito mode.
- Install privacy badger.
- Crumble the cookies, use Google-anon to remove cookies that Google uses to track you.
Thank You