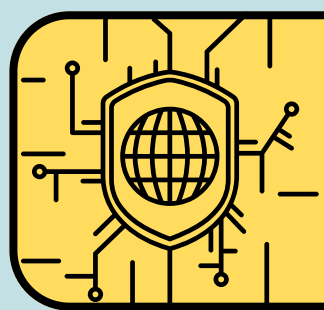




Basic Digital Safety

It is what we refer to as the proper approach to personal safety when using digital technologies. Online safety is being aware of the potential threats that you may encounter while using the Internet.

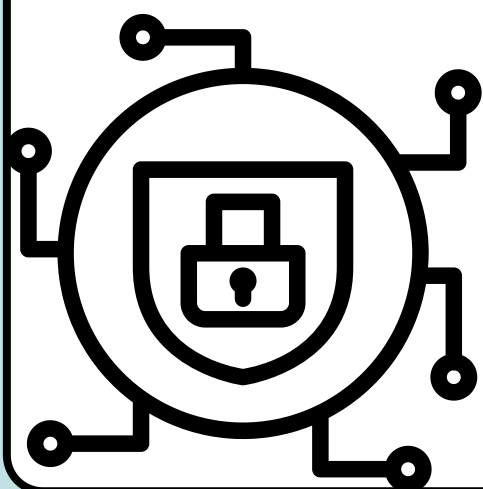
In today's increasingly digital world, safeguarding personal information and ensuring digital safety is crucial. Here are some fundamental principles to follow for maintaining digital security:

Strong Passwords

Use Complex Passwords: Make passwords that are at least 12 characters long and contain a mix of uppercase and lowercase letters, numbers, and special characters.

Passwords should be unique; do not use the same password for multiple accounts. Every account should have its own unique password.

Password Managers: A password manager can securely store and generate complex passwords, making it easier to manage multiple accounts.



Personal Information Protection:

Be cautious when sharing personal information online, especially on social media and unfamiliar websites.

Privacy Settings: Change the privacy settings on social media platforms and other online services to limit who can see your information.

Two-Factor Authentication (2FA): Turn on 2FA whenever possible to add an extra layer of security to your accounts by requiring a second form of verification.



Install reliable antivirus and anti-malware software to detect and eliminate malicious threats.

Firewalls: Configure firewalls to monitor and control incoming and outgoing network traffic, adding an extra layer of security.



Safe Browsing Practices.

Secure websites: Only enter personal information on websites with HTTPS, which indicates a secure connection.

Avoid Suspicious Links: Never click on links or download attachments from unknown or suspicious sources, as they could contain malware or phishing attempts.

Ad blockers: Use ad blockers to avoid malicious ads that can lead to dangerous websites or downloads.



Responsible use of public Wi-Fi.

Avoid Sensitive Transactions: Do not conduct sensitive transactions, such as online banking or shopping, on public Wi-Fi networks.

Use a VPN: Use a Virtual Private Network (VPN) to encrypt your internet connection and protect your data while using public Wi-Fi.

REFERENCES

K. Morris, "Teaching digital citizenship: 10 Internet safety tips for students (with posters)," March 2019, <http://www.kathleenamorris.com/2019/03/12/internet-safety/>