Online Safety and Security

Today, the digital world is as essential as the physical one.

Here are 10 tips about how to be safe online:

Enable Two-Factor Authentication (2FA)

Extra Security Layer

2FA adds a crucial second step to your login process, significantly improving account protection.

Thwarting Password Breaches

Even if your password is compromised, attackers can't access your account without the second factor (2FA).

Various 2FA Methods

Choose from SMS codes, authenticator apps, or hardware keys for use your second factor.

Navigate Secure Websites

1

Check for HTTPS

Always verify that the URL begins with 'https://' before entering sensitive information.

2

Look for the Padlock

A padlock icon in the address bar indicates a secure, encoded connection.

3

Be alert to warnings

Heed browser warnings about potential security risks or invalid certificates.

Use Strong, Customised Passwords

Length is important

Create passwords at least 12 characters long. Longer passwords are harder to decode.

Mix everything

Associating uppercase and lowercase letters, numbers, and symbols for increased complexity.

Use different passwords

Different passwords must be used for different accounts. With this method you can avoid a breach of an account

Attention of Phishing Attempts

1 **Check e-mail senders**

Check the e-mail address of the sender. Companies use official domain names.

2 **Beware of urgency**

Phishers often create a false sense of urgency. Check before accepting urgency.

3 **Check links carefully**

Use the mouse over links to preview URLs (Uniform Resource Locators) . Do not click on shady or unexpected links.

4 **Protecting personal information**

Legal organisations do not ask for sensitive data via e-mail or unprotected channels.

Update your devices regularly

1

Enable Auto-Updates

Configure your devices to automatically install updates when available.

2

Update All Software

Keep your operating system, apps, and antivirus software up-to-date.

3

Install Antivirus

Install critical security updates released to address vulnerabilities.

Back Up Your Data

Cloud Backup

Use reliable cloud services for convenient, off-site data storage.

External Hard Drives

Regularly back up to physical drives for local, offline storage.

Automated Backups

Set up automatic, scheduled backups to provide consistent data protection.

Avoiding Public Wi-Fi Networks

Risk	Attenuation
Data Interception	Use a VPN
Malware Distribution	Keep Firewall Active
Fake Hotspots	Verify Network Name
phishing actions	Use HTTPS Websites

Checking accounts online

1

Regular checks

Check account activity and transactions frequently to detect any shady activity.

2

Activate notifications

Set up alerts for access, purchases or changes to account settings.

3

Use of monitoring tools

Use identity monitoring services to recognise personal data on the web.

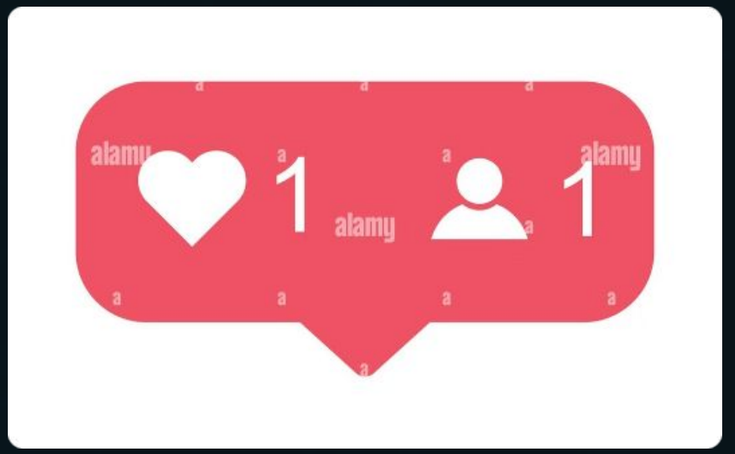
Being careful with social media

Regulating privacy settings

Review and update social media privacy settings regularly to control information sharing.

Think before posting

Always consider the consequences of sharing personal information or opinions online.



Accepting requests with care

Be selective with your contacts and avoid accepting requests from unknown persons.