

Internet connection:

Using encrypted networks will ensure online activity remains private. Avoiding using public WIFI for sensitive transactions and instead using a VPN to enhance security when browsing online internet.

Digital footprint:

Online activity can present more than you think. Therefore, regularly reviewing your social media settings would be helpful in the information you share. Examinations on a regular basis of your digital footprint can help maintain privacy.

Protecting passwords:

Creating strong and unique passwords will avoid accessible information like birthdays or common words. Regularly updating a password can help stay ahead of potential threats.

Safeguarding:

Be careful of who you share your passwords to online. Limiting identifiable information that you post on social media for example. Also ensuring privacy settings are configured to protect your data. When sharing sensitive data, always consider the possible consequences.

Stay Safe Online

Phishing Scams:

These are designed into tricking you into revealing personal information. Often used fake emails, messages or websites. These type of scams trick you into clicking on untrustworthy links or providing sensitive data such as passwords or credit card details. To protect yourself from potential threat you can verify the sender's identity, prevent clicking on suspicious links.

System Update:

Keeping a system updated. The crucial of keeping a system updated is ensuring operating systems, browsers and applications are always up to date.

Securing your internet protection:

Making sure to update on a regularly standard is a crucial way in protecting your personal information and ensuring all of your online activity is safe. Software is a crucial way of protecting your personal information. Enable automatic updates and ensuring that the person's software is remaining up to date with the latest security enhancements.

