

10 tips to stay safe online



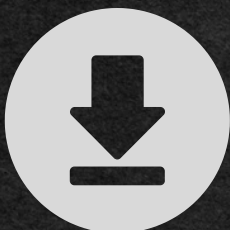
Select strong passwords that are harder for hackers to hack into.

If you use the same password for many accounts, your data may be compromised.



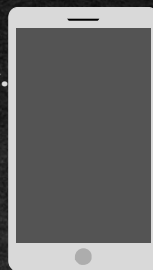
6. Be cautious while clicking any links.

A negligent click could expose your personal data online or infect your device with malware. It's important to use caution when browsing the internet and avoid certain types of content.



2. Take extra care when downloading anything.

Fooling you into installing malware that can be used to unlock a "backdoor" into your computer is one of the key objectives of hackers.



7. Verify that each of your devices is secure.

It's crucial that mobile devices are properly secured because up to 60% of consumers do their online shopping and information research on them rather than desktop PCs. Using passwords, passcodes, and additional security features like fingerprint readers or face-scanning technology to secure all of your devices is a good idea. If you follow these procedures, the chance of a cyberattack or hackers obtaining your personal information will decrease.



3. When possible, enable multi-factor authentication.

To access an online account, users must successfully complete two or more multifactor authentication verification steps (MFA).



8. Regularly backup your data.

Regularly backing up your data to external hard drives is crucial. You will always have a copy of the most important things in case something happens to it or it gets misplaced.



4. Update your operating systems and software regularly.

Developers constantly monitor the most recent threats to the security of their products and provide security updates to address weaknesses in the software.



9. Verify that you are always using a secure internet connection.

However, since you have no control over the security of public Wi-Fi and are open to cyberattacks, it is not recommended.



5. Watch out for people you meet online.

Not all people you meet online are who they claim to be. They could not possibly be real, in truth. Phishing social network profiles is a common tactic used by hackers to draw in innocent internet users and obtain their personal data.



10. Verify if the websites seem and feel secure.

It's vital that every website you visit be legitimate, especially e-commerce sites and other sites where transactions take place.

Watch out for URLs that begin with HTTPS (which stands for "secure") rather than HTTP.