

10 tips to stay safe online



1. Choose strong passwords that are more difficult for hackers to crack

Your data could be compromised if you use the same password for several accounts



2. Always make sure you are connected to a secure internet connection

However, using public Wi-Fi is not recommended as you are vulnerable to cyberattacks and have no control over its security.



3. Enable multi-factor authentication where is possible

Users must successfully complete two or more multifactor authentication verification processes in order to access an online account (MFA).



4. Always keep software and operating systems updated

Developers always keep an eye out for the latest threats to their products' security and offer security updates that fix any weaknesses in the program.



5. Check if the websites look and feel secure

It's critical that every website you visit be genuine, especially those where you transact (like e-commerce sites). Better lookout for URLs that start with HTTPS rather than HTTP (the S stands for "secure")



6. Be careful when you click on a link

One careless click could put your private information online or infect your device with viruses. It is crucial to browse carefully and stay away from some kinds of internet content



7. Make sure that your devices are all secure

Up to 60% of consumers use their mobile devices instead of desktop computers for online shopping and information research, so it's important that they are well secured. It is a good idea to secure all of your devices with passwords, passcodes, and extra security features like fingerprint readers or face-scanning technology. The probability of a cyberattack or hackers getting your personal data will drop if you take these precautions.



8. Back up your data regularly

It is very important to back up your data on external hard drives regularly. If anything happens with it, or it gets lost, you will always have a copy of the most important things



9. Be very careful on what you download

One of the main goals of hackers is to trick you into installing malware that can be used to open a "backdoor" to your computer.



10. Be careful who you meet online

Not everyone you meet online is who they say they are. In fact, they could not even be real. Hackers often use fake social media profiles to attract unaware internet users and steal their personal information.