

Basic Digital Safety



- **Refrain from using public Wi-Fi to access personal or financial data.**

Although it may appear obvious, many individuals still access their bank accounts or use their credit cards to make transactions while connected to public Wi-Fi, which can be risky. It's most optimal to carry out those tasks on a safe and secure connection.

- **Turn off any unnecessary items.**

Hackers have the ability to exploit specific functions on your phone to access your data, whereabouts, or network. Therefore, rather than leaving your GPS, wireless connection, and location tracking activated continuously, simply enable them only when necessary.

- **Choose your apps wisely.**

Make sure to only install applications from reputable sources known for their good reputation. Ensure that you regularly update your software and apps while removing any unused old apps.

<https://www.chubb.com/us-en/individuals-families/resources/6-ways-to-protect-yourself-from-hackers.html>

- **Make sure you are using a secure internet connection.**

While it is advised against, there are instances when using public Wi-Fi is inevitable while on the go. Nevertheless, if you access the internet while in a public area and connect to a public Wi-Fi network, you do not have complete control over its security, making you susceptible to cyber threats. Therefore, when using public Wi-Fi, refrain from conducting personal transactions involving sensitive information like online banking or online shopping.

- **Make sure your devices are protected.**

It is crucial to ensure that mobile devices are secured properly, especially since up to 60% of individuals use them for shopping and accessing information online instead of desktops. It is recommended to use passwords or passcodes along with other security features like fingerprint readers or face-scanning technology on all your electronic devices such as phones, computers, tablets, smartwatches, and smart TVs. These steps will decrease the chances of a cyberattack or hackers stealing your personal information.

- **It is important to exercise caution when connecting to free Wi-Fi hotspots.**

Unsecured free Wi-Fi networks make it possible for hackers to monitor your online activity. Utilize a VPN to safeguard your connection while using a public Wi-Fi network.

<https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online>

- **Increase your knowledge by educating yourself about online scams.**

It is crucial to learn about online scams in today's modern digital era. Staying informed is crucial in order to outsmart scammers who are always coming up with new tricks. Familiarize yourself with the indications of typical scams, such as receiving unsolicited emails requesting personal details or being tempted by offers that appear too good to be true.

- **Make sure to regularly update your software.**

Frequently updating your software is crucial for staying safe online. These frequent updates typically contain security patches that defend against emerging threats. Additionally, make sure to activate automatic updates on all your devices so you are always running the most current and secure versions. Taking this easy measure can significantly decrease the chances of digital attacks targeting you.

- **Create passwords that are both strong and unique to enhance your security.**

Having strong and distinct passwords serves as a secondary form of protection on the internet. Refrain from using commonly used words or easily guessed information such as your date of birth. Instead of that, combine letters, numbers, and symbols to generate a complicated password. Additionally, it is wise to use unique passwords for every account. This way, if one is hacked, the rest remain secure. Recalling all of them may appear difficult but, these tools ensure the security of your passwords and facilitate safe access to your accounts. Setting difficult passwords greatly decreases your chances of being hacked. If you believe you have witnessed a scam, do not stay silent. Informing acquaintances can increase awareness of scams and prevent people from becoming victims.

<https://www.dunbareducation.com/blog/2024/01/top-tips-for-internet-safety?source=google.com>

https://www.google.com/search?q=warning+tips+for+online+scams&rlz=1C1VDKB_enGB1033GB1034&oq=warning+tips+for+online+scams&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICA EQABgWGB4yCggCEAAyAQYogQyCggDEAAyAQYogQyCggEEAAyAQYogQyCggFEAAyAQYogTSAQkzMDA4N2oxajeoAgCwAgA&sourceid=chrome&ie=UTF-8