Popular threats on iOS and how to avoid them

AVAST CYBERHOOD WATCH **TOOLKIT**

Popular threats on iOS and how to avoid them

For a long time, Apple's iOS was considered immune to malware, however recent attacks have proved this illusion of invulnerability isn't what it used to be. iOS devices are certainly less likely to contract malware than their Android counterparts, but it can occur. In this guide, we'll single out the most common threats that can affect iOS devices and explain what you can do to prevent them.

Unlike Android devices, app-based malware is less common on iPhones and iPads. This is because iOS users download their apps from the App Store which uses some of the most robust security measures around. iOS apps are also heavily sandboxed, which means they cannot interact with other apps or the operating system itself. However, an iOS device that's had the limitations imposed by Apple and other third parties removed, is at much greater risk.

Despite their strong security, iOS devices are equally vulnerable to browser-based attacks such as phishing. This is a cybercrime technique carried out through electronic communications such as email or text that uses fraud, trickery or deception to trick people into disclosing sensitive personal information.
Another potential vulnerability is public Wi-Fi connections with weak security. These open networks are unencrypted, meaning anyone connected to them can see what you're doing online and steal your data, such as credit card information.

To prevent cybercriminals from launching phishing attacks on your iOS device and snooping on your online activity, consider the following:

1. Question everything about the sender and the content of a message you receive. Does the sender's address look official or suspicious? Does the message seem too good to be true? Often, cybercriminals claim to be someone they're not and use 'fear of missing out' techniques to trick you

2. Are there punctuation and grammatical errors, and is there an over-dramatic sense of urgency and emotion in the message? The use of threatening language and false claims that make you panic, fearful, hopeful or curious are common tactics

3. Make sure your software is always up-to-date

4. Install a strong antivirus with a Virtual Private Network (VPN). These are essential tools for keeping your phone safe from phishing attacks and unsecured WiFi networks