KnowBe4

Security Hints & Tips

How Secure is Your Mobile Device?

Most of us have a smartphone, but how many of us really think about the security threats faced by these mobile devices? Mobile devices are vulnerable to many different types of threats. Scammers are increasing their attacks on mobile devices and targeting your phone using malicious applications. Using these methods, they can steal personal and business information without you having any idea what's going on.

Even if you've downloaded a security or antivirus application, securing your smartphone goes beyond these services. Improving your mobile security practices is your best defense against the privacy and security issues associated with your mobile device.

How can I improve my mobile security practices?

Always remember these best practices to minimize the risk of exploits to your mobile devices:

1. **Ensure your phone's operating system is always up to date.** Operating systems are often updated in order to fix security flaws. Many malicious threats are caused by security flaws that remain unfixed due to an out of date operating system.
2. **Watch out for malicious apps in your app store.** Official app stores regularly remove applications containing malware, but sometimes these dangerous apps slip past and can be downloaded by unsuspecting users. Do your research, read reviews and pay attention to the number of downloads it has. Never download applications from sources other than official app stores.
3. **Ensure applications are not asking for access to things on your phone that are irrelevant to their function.** Applications usually ask for a list of permissions to files, folders, other applications, and data before they're downloaded. Don't blindly approve these permissions. If the permission requests seem unnecessary, look for an alternative application in your app store.
4. **No password or weak password protection.** Many people still don't use a password to lock their phone. If your device is lost or stolen, thieves will have easy access to all of the information stored on your phone.
5. **Be careful with public WiFi.** Scammers use technology that lets them see what you're doing. Avoid logging in to your online services or performing any sensitive transactions (such as banking) over public WiFi.

The KnowBe4 Security Team