6 Tips for Increasing Smartphone Security

Devolutions

SMARTPHONES ARE MORE LIKE MINICOMPUTERS

Smartphones have changed...well, everything! They've changed how we work, how we interact with each other, how we order pizza *(mmmmm pizza)*, how we book flights, how we play games — and the list goes on.

Thanks to their processing capacity, connectivity and countless applications, smartphones are more like minicomputers that you can take with you everywhere, while still using to make calls. Now think about all the information you have on your phone, from emails to texts, and phonebook entries to pictures. Your phone holds a plethora of personal information that's potentially accessible to prying eyes...or ears.

However, because smartphones are so convenient and we use them throughout the day (and sometimes throughout the night!), we tend to overlook security. This puts our private and sensitive information at risk of falling into the wrong hands.

The good news is that we can become less of a target for hackers and snoopers by following some basic security hygiene tips:

1. Avoid Having Confidential Conversations in Public

I've lost track of how many times I've been sitting in an airport, coffee shop, restaurant, or some other public place and overheard (not on purpose of course!) someone reveal something staggeringly personal and private while talking on their smartphone. Don't forget that someone could be eavesdropping on your conversation!

And so, our security hygiene tip here is: never discuss anything confidential in public. This doesn't just include obvious topics like passwords. It also includes things like vacation plans, or even sharing your recent Amazon purchase (because someone might race to your house and grab it from your porch before you get home!). You shouldn't be paranoid that "Big Brother" (or make that "Big Hackers") is constantly listening to you, but you should use common sense and err on the side of caution.

2. Beware of Fake Texts

Hackers are notorious for sending out fake text messages that direct you to a website or ask you to open a document. Yes, most of these texts are ridiculous and you send them straight to the trash. But some of them look very authentic, and appear to come from people and (especially) companies you know and trust.

The advice here is: when in doubt, delete the text or (if you wish) confirm the authenticity by making a call or sending an email. Just be careful that you don't use the number supplied in the text, because that may also be phony.

3. Beware of Fake Emails

Hackers are surprisingly good at creating attention-grabbing subject lines that compel people to open emails (e.g. "confirming our 3pm meeting" or "your package is delayed – details inside"). You need to exercise the same caution and diligence here as you do when using your desktop or laptop. The best option is to delete suspicious emails. But if you open them up, at the very least don't click any links or download any attachments.

4. Only Download Apps from Trusted Sources

Who doesn't have 35 applications or more on their smartphone?! These days, we have apps for everything: games, social media, weather — and much more. But the bad news is that hackers are also using apps to spread malware. To avoid getting victimized, install the latest software updates and security checks on your smartphone and only download applications from trusted sources (e.g. App Store, Google Play, etc.).

5. Store Your Smartphone Properly

If you're in a public place, never leave your smartphone in a bag or purse on the floor, because it's very easy for thieves to steal it — all they need is a few seconds. It's also not a great idea to keep your smartphone in your back pocket.

In addition to properly storing it, don't forget to configure your smartphone so that it locks or turns off automatically after a period of inactivity (make it a short period!), and require a password, PIN or sequence to unlock your phone. Encrypting your data is also a wise move, and you should have the ability to locate a lost device and delete data remotely.

6. Use Secure Wi-Fi Connections

Only connect to the Internet through secured Wi-Fi access points. If this isn't possible, then use a reputable VPN to encrypt your data and keep your activity hidden.

The Bottom Line

Smartphones are essential. Seriously: I can barely breathe if I don't have my smartphone with me! But we need to be careful with the things (and the people) we love. Controlling access with a password, installing legitimate apps, and using secure remote access can prevent your private information from falling into the wrong hands. Like I always say, better to be safe than sorry!