5 Smartphone Mistakes and How to Avoid Them

It's tough to remember how we got by before smartphones. How did we get around town without handy access to Google Maps? Pay our bills on time before we had credit card and banking apps? Or let someone know we were running late without text messaging?

Because completing tasks on smartphones is so easy, we tend to overlook the sensitivity of the data we store on them. This can put our information at risk. Below are five mistakes that most of us make when using our smartphones and some simple best practices for avoiding these pitfalls.

Mistake #1: Not auto-locking your phone or using a password
Surprisingly, most smartphone users don't password-protect their devices, making information stored on them vulnerable if phones are lost or stolen.

The fixes

- **Set your phone to auto-lock at the minimum time offered**—for iPhones, that's one minute, and for Droids, that's 15 seconds.
- **Change your settings to immediately required your passcode when unlocking your phone**
- **Opt for a PIN or password instead of using a screen-lock pattern to lock and unlock your phone.** Although having a password is only the most basic form of security, it may at least buy you some time and give you the opportunity to remotely wipe or track your phone if it is lost or stolen.

Mistake #2: Connecting to public or unsecure Wi-Fi networks
Public Wi-Fi and also be sure that your auto-discovery is turned off if your phone has that function. This will prevent your phone from automatically connecting to the first open Wi-Fi network it locates.

If you absolutely need to connect to public Wi-Fi, don't send personal or payment information over the network. And when you're done using it, go to your phone's settings and have it "forget" the network, which stops your phone from automatically reconnecting to the network if it detects it again.

Mistake #3: Using out-of-date apps and software
Outdated apps and mobile operating system software leave your phone open to security vulnerabilities.

The fixes

- **Keep apps up to date.** This patches holes that bad guys might exploit to access your data. Most smartphones have an automatic update option for apps, so be sure to use it!
- **Update your mobile OS software** as soon as you receive notification that an update is available.

Mistake #4: Staying logged into apps that store your financial information (e.g., shopping or banking

service providers)
Although certainly more convenient than entering your credentials every time you need access, this habit could leave you vulnerable to serious financial risk. If your phone is lost, stolen, or remotely accessed over a Wi-Fi network, you're basically handing the bad guys your wallet.

The Fix: Don't stay logged into apps, and clear your device's browser history regularly.

Mistake #5: Clicking on links sent though unsolicited texts or e-mails
Cyber criminals have crossed over from the desktop to the mobile world. They now deploy their phishing attempts through text messages or e-mails, hoping that you'll click on their bogus links and provide them with your credentials or financial information.

The fix: Be just as wary of clicking links and downloading attachments on your smartphone as you are on your desktop and laptop—don't do it. If the links or attachments come via e-mail or text messages from individuals or organizations you don't know, consider them fraudulent until you can verify the senders. It's not unheard of these days for viruses to infect smartphones.

What the future holds
All signs point to more of us using mobile devices to communicate and transact business, which means that more of our information will be out there tempting hackers to steal it. Don't be lulled into a false sense of security. Follow the advice shared above. Remember, when it comes to cyber crime today, it's now no longer so much a question of *if* you will get hacked, but *when*.