SAVVY TRAINING
& CONSULTING

Tips for Securing your iPhone

We like to share good information when we come across it.

Kelly Sheridan, Staff Editor at Dark Reading, shared her *Top 10 Tips for Securing Your iPhone* in a recent web post. Sheridan begins with an important question. "[A]re our iPhones as secure as they could be?" Although Apple provides a set of development protocols called "App Transport Security (ATS)," not all apps use it. View the full post here for more information, examples and technical background.

Here are tips you can immediately put in place.

1. **Remove apps you are no longer using**. Not only do they take up space, but they could be a security risk since apps that are not maintained may not be receiving security updates and fixes.
2. **Update your device to the latest release of the mobile operating system**. By design, "these updates... often fix critical vulnerabilities," according to Sheridan.
3. **Choose carefully which apps need access to data on your device.** "Why does my flashlight need my location? It doesn't. Many third-party apps often request permission to access iPhone features and data they don't truly need," says Sheridan. Go into *Settings > Privacy* to view which apps have access to things such as your contacts, calendar or photos. Drill down into *Location Services* to disable location-sharing as appropriate for each app.
4. **Create an alphanumeric passcode.** Even if you are using biometric data, such as facial recognition or a thumbprint, a secure passcode remains important. Go to *Settings > Touch ID & Passcode* (or *Face ID & Passcode*) and then go to *Change Passcode* and tap *Passcode Options* to view the option for *Custom Alphanumeric Code*. Even though you already know this, we remind you not to share your passcode with anyone else, and don't add another person's biometric data to your device.
5. **Multi-Factor Authentication.** Yes, we agree it's annoying. But unfortunately, it's necessary and a strong defense against hackers, especially when you use unique passwords for all of your mobile apps.
6. **Set Login Limits**. If someone is trying to access your device, the device can automatically erase all data after 10 attempts. This setting is found in *Access Settings > Touch ID & Passcodes*. Scroll to the bottom and toggle *Erase Data* to the On position.

7. **Prevent Cross-Site Tracking**. Some websites use this to monitor your online activity. Remember looking at that rice cooker and it suddenly appeared on your Facebook feed? That's what's happening. Go into *Settings > Safari* and scroll down until you see *Prevent Cross-Site Tracking* under the *Privacy & Security* group. Turn that On to prevent advertisers from collecting your browsing data.
8. **Be Careful Where You Click**. Watch for links that appear suspicious or come from unknown sources. [If you need a training resource on phishing, contact us for more information about our partner, KnowBe4.]
9. **Remove Tracking Data from Images**. Pictures can contain hidden tracking code that tells companies whether an email was opened. "One of the tips I recommend for iPhone users is to disable download images in the email setting as this can leak sensitive information about your device, browser, and location," says Joseph Carson, chief security scientist and advisory CISO at Thycotic. "It is enabled by default, and disabling it puts you back in control of that by choosing which images you want to download." In addition, you can turn off the location in photos you share by clicking on *Options* and switching off *Location* when sharing with others.