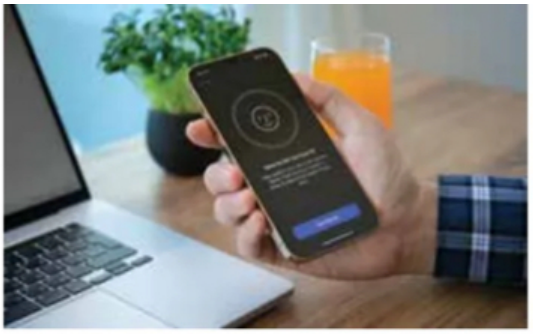

Photo by DenPhotos

IPHONE SECURITY TIPS

Our iPhones store sensitive personal data, including pictures, private chats, passwords, and credit card information. Despite their security features, hackers still attempt to access this data.

The National Security Agency (NSA) has shared best practices for mobile device security. Here are some of the best tips:

1. Avoid public Wi-Fi networks. They lack authentication and encryption, making them vulnerable to interception by hackers.
2. Use a strong passcode. Default passcodes like "123456" or "000000" can be easily learned by observing how you unlock your iPhone. Consider using a longer passcode or a passcode with special characters. Avoid using birthdays or anniversaries as passcodes, as thieves can access this information if they steal your wallet and iPhone. Instead, use random numbers. While it may be challenging to remember, it's more secure. I
3. To change your passcode, go to Settings > Face ID & Passcode > Change Passcode. After entering your current passcode, tap on Passcode Options and choose Custom Alphanumeric Code.
4. Use biometric authentication like Face ID or Touch ID for added security. Both methods are convenient and prevent access to sensitive data like hidden albums, locked apps, or in-app purchases.
5. To enable Face ID or Touch ID, go to Settings > Face ID & Passcode and set up Face ID.
6. Your iPhone can share location with any app, but not every app needs access, especially not your exact location constantly. The NSA recommends ditching Location Services and only using it when necessary.
7. Keep apps to a minimum. This reduces storage, improves battery life and performance, and makes you feel safer.
8. Only download apps from official app stores, especially if you're an Android user or iPhone user in the European Union. Reputable companies like Trello and Evernote are good options. When you find an app you like, check the Data Linked to You section at the bottom of the App Store page to see what data the app may collect.
9. Don't trust pop-up messages when browsing the web. They're usually unwanted and can be a sign of a security issue. Avoid tapping pop-up messages unless certain. Some may be ads, but it's best to avoid them, especially if they seem shady. If that happens, close all applications and delete untrustworthy apps to see if it fixes the issue.

Turn off your iPhone at least once a week for privacy against zero-click attacks. These attacks can execute code inside your iPhone or access your information without your knowledge. Turning off your iPhone once a week is quick and easy to prevent this. It may also improve your iPhone's performance.

Avoid tapping links or opening files from unknown sources. These links often contain malware that can control your iPhone, access your accounts, or access your information. Unless you completely trust the message, avoid opening any link or file. If you're unsure, contact the sender using a different method to verify their identity.

KEEP YOUR IPHONE UP TO DATE FOR SECURITY

Updating your iPhone offers several benefits. Apple may release a new patch to fix a vulnerability you weren't aware of, and updates improve security. You might also get new features. There's no reason not to keep your iPhone up to date. You can install security updates if you don't want a new iOS version. To ensure the latest software update, go to Settings > General > Software Update and check for an update.

JEFF BOHR
Naples Mac Help

Jeff is your one-stop Mac expert, an Certified Support Professional, and 37-year Mac user.
He can be reached at jeff@jeffbohr.com or 239.595.0482