Privacy Tips for Your iPhone

1. **Use two-factor authentication!** If you're running iOS 12 or later, go ahead and sign up for TFA on websites you visit. Those sites will send you a confirmation text when you sign in, and your iPhone will automatically copy that confirmation code into your web browser, making 2FA a breeze.

2. **Don't re-use passwords!** Go to Settings > Passwords & Accounts > Website & App Passwords. You'll see all the passwords your iPhone has saved to your Keychain. Any password with an exclamation mark in a triangle next to it is used on more than one site. You should make these unique! Tap to change that password.

3. **Use strong passwords!** When you use your iPhone to generate a password for a website, top the "Use Strong Password" to make a better password. iOS will automatically save it in your keychain, so you don't have to remember it. Stronger passwords means that if a website gets their database hacked, you'll be safer.

4. **Use Safari!** By default, it will stop advertisers from tracking you around the web, slow down Facebook and Google, and stop websites from requesting your device's unique digital signature.

5. **Audit and block apps that have access to your camera, microphone, and location!** Go to Settings > Privacy to see a list of these things, then tap on a category to see which of you apps have access. For apps that don't really need access to, say, your location or your microphone, cut them off!

6. **Search using DuckDuckGo!** Their business model doesn't rely on collecting data about you, and so they don't. Go to Settings > Safari > Search Engine and tap on DuckDuckGo. Their results are just as good as Google.

7. **Be ready to turn off Touch ID and Face ID!** Thanks to the Fifth Amendment, law enforcement can't compel you to give up your passcode. But they can compel you to unlock your phone using Touch ID or Face ID. Go to Settings > Emergency SOS and turn on "Call with Side Button." Now, when you press your iPhone's side button five times, only your passcode will open your phone.

8. **Delete lockscreen widgets that display person info!** Swipe to the right and see what widgets you have available who picks up your phone. If there are any that display personal info (like your calendar), scroll down to tap "Edit" and remove them. Similarly, go to Settings > Touch ID & Passcode and look for "Allow Access When Locked." Disable any feature you don't want strangers to access.

9. **Don't show strangers your messages!** Go to Settings > Notifications > Messages > Show Previews, then select "When Unlocked." Otherwise, incoming messages are readable on your lock screen to anyone holding your phone.

10. **Enable Find My iPhone?** Go to Settings > Apple ID > iCloud > Find My iPhone. Enable this if you'd like the ability to wipe your phone remotely, if it gets stolen. Disable this if you're more worried about Apple knowing where your phone is.

Sources: Fast Company and Life Hacker.