TECKPATH
your strategic partner in IT

5 Things You Can Do Today To Keep Your Mobile Device Safe

TECKPATH
your strategic partner in IT

Overview

Your mobile device has a lot of sensitive information on it, and it's increasingly becoming a target for cyberattacks. While you should always be careful about what you download on the device, there are some simple things you can do today that make it very difficult for an attacker to steal anything off your device.

Here are 5 things you can do today to keep your mobile device safe:

1. The silly things we do with passwords. Did you know that people actually "hide" their passwords in their smartphone's contacts app? Many people don't realize that what they're doing is actually quite the opposite of "hiding." In fact, a large amount of applications, not to mention malware, actually access contacts.

In this section you can find information about the importance of password security and actionable advice on keeping those passwords for your eyes only.

2. The case for not jailbreaking/rooting your device. You may have heard that jailbreaking or rooting your device will let you use your phone internationally, or on other carriers. There are a lot of reasons people may jailbreak their device, but there are also a lot of security concerns people may not realize they're running into.

We'll tell you more about jailbreaking/rooting, and why it's risky.

3. The real story behind those software updates. Updating your phone can be annoying. It takes time and it mostly just looks like "bug fixes" and "feature improvements." But there's a deeper story to be told here.

We'll tell you more about what's really behind those OS updates and why you need to keep up with them.

4. The problem with public Wi-Fi. You're at the airport when you realize you forgot to download that eBook before you left home. Maybe you're stuck in line at a coffee shop, low on data, and really want to check Facebook. Connecting to public Wi-Fi might be convenient, but it's not a safe place.

In this section you can find information about what a "Man-in-the-Middle" attack is, and how it could affect your personal and corporate data.

5. The ways we accidentally give over our information on mobile. While there are a lot of parallels to the PC, mobile devices offer a different kind of experience when viewing emails, media, and messages. This also means it's sometimes a little harder to tell when a communication with you is legitimate or not.

In this section you can find information about phishing attacks on mobile, and how to avoid getting duped.

[1]Stay Safe Online, "National Cyber Security Awareness Month", National Cyber Security Alliance 2015

1. The silly things we do with our passwords

It's hard to remember the myriad of passwords we use for our accounts online. There are a number of ways we hear of people dealing with this: writing them down on a piece of paper, using the same password across all your accounts, etc.

One of the most concerning practices we've heard of, however, is storing your passwords in your mobile contacts.

This is a definite "don't do," in our books.

I'm hiding them in there!

One of the main justifications we've heard for storing your passwords as contacts is that you're actually "hiding" them in there. Have you ever "hidden" a file in a file in a file on your PC in the hopes that it'd be hard for someone to find it? It's a similar mentality.

But you're not actually hiding them at all.

Apps accessing contacts

There are tons of legitimate apps that actually access contact information. Your social networks do it, your shopping apps do it, your health apps do it. Most of the time apps use your contacts in order to help you find friends or invite new people to the service. While the intentions are good, you might wind up sharing all of your passwords with the developers of the apps on your phone.

Suddenly, you don't know how your passwords are being stored, who has access to them, and if the systems they're living on are protected from attack.

But seriously, remembering all those passwords is a chore

We get it, many people have upwards of 100 accounts online and you always hear the advice, "Use a different password for all your important accounts!" There are tools that can help. 1Password and LastPass are online password management tools that store all of your passwords and let you use one password across all your accounts.

Of course, no system is perfectly secure and any time you store data online, you run the risk of losing that data. However, the benefit of storing your passwords in a safe, managed service hugely outweighs the risk of storing them in your contacts.

2. The case for not jailbreaking/rooting your device

Jailbreaking your iOS device (or rooting in the case of Android) is tempting. After all, who wouldn't want access to a whole new world of apps, easier international travel, and more control over their phone?

If you've felt the lure to read the latest jailbreaking/rooting tutorial and take the plunge, you're not alone: An estimated 7.5 percent of all iPhones[2]—amounting to more than 30 million devices worldwide—are jailbroken. Jailbreaking is especially popular in China, where an estimated 13 percent of all iPhones are jailbroken.While we understand the temptation, we have one piece of advice:

Unless you're a pro, avoid jailbreaking

There are many security concerns you might not realize if you jailbreak / root your device. In many cases you may need to change some security settings on the device in order for the jailbreak to work. Those who don't know what they're doing, however, may not know how to properly reinstate security settings after the jailbreak is complete, leaving themselves open to attack.

People with jailbroken phones will also readily download third-party apps. Though this is possible to do on non-jailbroken devices, it is much easier to accomplish in a jailbroken environment. Apps on a jailbroken device can also run with escalated privileges and access sensitive data belonging to other apps.

For example, the recent KeyRaider malware impacted jailbroken iOS devices and stole 225k Apple accounts.

It's not just about security

Outside of security, there are many other reasons to be wary of jailbreaking or rooting your phone. For one, you'll likely kiss any built-in customer support or warranty goodbye, which is problematic if you ever have a problem with your phone (and potentially out of several hundred dollars). It can also wreak havoc on battery life, and make your phone inoperable with future operating systems.

So, to keep your phone safe and running optimally, stay far away from jailbreaking/rooting. It might be less fun coloring in between the lines, but it's one of the best things you can do for your phone and data.

[2] Daily Tech, "'WireLurker' Malware May Have Infected 100,000+ iPhones, No Jailbreak Required", Jason Mick, November 2014

3. The real story behind these software updates

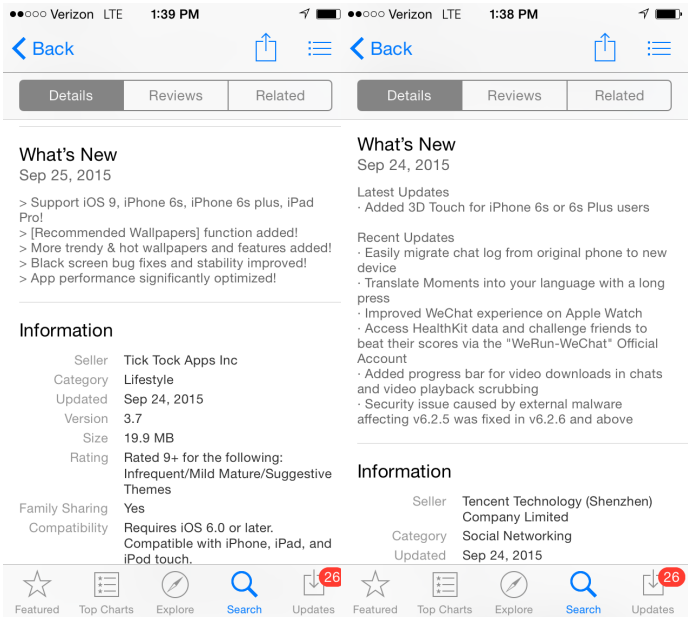
Updating your software is sometimes an inconvenience, but it's also necessary to keeping up your mobile security hygiene.

Sometimes updates require connecting to a power source, backing up data, or temporarily losing access to an app or service while the update processes. Whatever the reason, oftentimes we see that little tally of available updates increase and increase.

The problem is, there are many critical security fixes that get pushed through these OS and app updates and when we ignore them, we leave ourselves vulnerable and open to attack.

It just says "bug fixes" and feature upgrades, why should I care?

Those "release notes," or the details that show you what you're getting in a software update don't often tell the whole story. Take, for example, these updates:



These are real release notes in the "What's New" section from apps affected by a piece of malware called XcodeGhost. The updates, though, just look like run-of-the-mill feature changes. In the first image you only see "Support for iOS 9." This is vague and it doesn't mention anything about security, but, in fact, the app had updated to get rid of the malware.

In the second screenshot, listed at the bottom of the notes, you see a more detailed reference to, "Security issue caused by external malware affecting v6.2.5 was fixed in v6.2.6 and above." This also references XcodeGhost and an update to get rid of the malware.

Latest and greatest

You always want to be running on the most up-to-date software on your device. In the security industry, when software is "patched," that often means researchers can publish their findings -- meaning bad guys and good guys alike suddenly have more information about vulnerabilities and other problems. Releasing this information is a good thing because it helps security teams learn how to secure their software, but it also means that people need to download the latest patches to make sure they're safe.

4. The problem with public Wi-Fi

We've all been there: you're running low on data, but you're stuck in a really long line and want to check Facebook. Maybe you're at the airport and realized you didn't download that eBook for the plane.

Unfortunately, connecting to and using that public Wi-Fi may be jeopardize your data and privacy.

Isn't it fine if I'm only there for a minute?

When you use the Internet, you're sending communications between computers. Accessing Facebook? Your phone is effectively talking to Facebook. The problem with public Wi-Fi is something called a "Man-in-the-Middle Attack," whereby an attacker can sit on the Wi-Fi connection and eavesdrop on this conversation.

In this attack, a person is able to listen in on an unprotected network, intercept your communications, and decrypt them (if they're even encrypted in the first place) to read what you're talking about.

I don't have anything interesting to say, so I'm safe

Downloading a book? You probably had to enter in your username and password. This counts as a communication that can be intercepted. Did you quickly enter your credit card information on Amazon? That counts as well. Send off a last-minute work email that may have included sensitive info? That, too. We oftentimes don't realize the kind of information we access or input on our mobile devices, but these phones and tablets are with us all the time. They access all kinds of personal data we should want to keep close to the chest.

Am I not supposed to use public Wi-Fi then?

In a way, yes. If you can avoid hopping on that free network, do. However, there are safe ways to surf the Internet while you're on the go! Use your 4G/LTE networks -- they are much safer than public Wi-Fi. If you want to work at a coffee shop with free Wi-Fi, use a VPN to encrypt your traffic.

If all else fails, avoid any transactions over public Wi-Fi that may involve signing into an account, checking email, or paying for something. Your data with thank you for it.

5. The ways we accidentally give over our information on mobile

Smartphones are pretty great, aren't they? They're small, portable and give us access to a world of information literally in our pockets.

But mobile devices' small form also means we interact with them pretty differently than desktop computers. In fact, studies have shown[3] that users are 3x more likely to click on a malicious link from their smartphone than a PC!

Focus on Visibility

We've all received phishing emails: they are typically designed to look like messages from banks, credit card companies, and similar organizations. The emails often have urgent subject lines requiring action to lure you to a phony website that looks—at least on a cursory glance—legitimate. Think: "Please verify your account" or "2nd Collections Notice."

After clicking on the link and believing that you've landed on the organization's actual website, you may enter in your username and password—unknowingly disclosing your private information to scammers.

Tricky business

While phishing isn't new, it does have unique repercussions when you receive malicious communications on mobile—and attackers know this. For one, it's hard to see if a link is actually legitimate. On a PC, you can hover over a link to determine if it will redirect to a suspicious looking address, but on mobile that's not the case.

It's also harder to spot if you're on a suspicious website, if you do end up clicking through. For instance, if you're on a large monitor you may pick up on a URL reads "usbanki.com" instead of "usbank.com," but on a mobile device it is much more difficult to spot this distinction. On PC you can also look for the "HTTPS" at the front of a URL, indicating that it is using a secure connection, but this is also not immediately evident on mobile where you have to click on the address bar and scroll to the front of the URL to determine if the site uses HTTPS.

Even incredibly tech-savvy people can fall prey to these schemes. The result? Your sensitive information gets in the hands of attackers who will likely use it for their gain.

Don't get phished–get savvy

To avoid getting phished on mobile, the best thing is to avoid clicking on email messages and links that just don't look right. Messages requesting your password, login details, or other important financial information should especially raise red flags. Know that your favorite social network, bank, or insurance company—basically any company that deals with sensitive information—will never ask for your password or other personal data via email.

[3] Security Intelligence, "Mobile Users 3 Times More Vulnerable to Phishing Attacks", Mickey Boodaei, January 201