Top 10 ways to secure your mobile phone

Help and Support

Help Desk

Homepage

Seems like everywhere you turn, there's news of another mobile security breach. Just last month, vulnerabilities in iOS 9.3.5 were being exploited by the notorious NSO Group, maker of surveillance software, to read text messages and emails, record sounds, collect passwords, and even track the calls and whereabouts of users. Apple released a security patch on August 25 in response.

Meanwhile, on the Android side, a Linux bug first introduced in Android 4.4 (and present in all future versions) left 1.4 billion users vulnerable to hijacking attacks. The vulnerability allows attackers to terminate connections and, if the connections aren't encrypted, inject malicious code or content into users' communications. Representatives from Google say they are aware of the vulnerability and are "taking the appropriate actions."

These hacks aren't happening in a vacuum. Mobile malware is a frontier ripe for cybercriminal activity. According to a 2015 Pew Research Center Report, nearly two-thirds of Americans own a smartphone, and roughly one in five of those users conduct most of their online browsing using their phone instead of a computer. The reality is that as more and more people use their phones to go online, more cybercriminals will hear the call.

Mobile malware on the rise

"Mobile malware has been on the rise drastically in last couple of years," says Nathan Collier, Senior Malware Intelligence Analyst at Malwarebytes. "Everything from backdoor malware that steals personal information to ransomware that locks your phone until payment is made exists in the mobile space. With millions of malware samples in the wild, there is no reason not to be concerned."

In addition to an increased volume of people turning to their phones as the primary means for going online, there's also an increase in using mobile devices for storing and transmitting sensitive data. The 2015 Pew Research Center Report also shows a full 57 percent of smartphone users doing their online banking on their phones.

But online banking is just the tip of the iceberg. GPS programs can find your location. Mobile apps often require that you allow them to access data stored in your phone or on the cloud. You can receive digital boarding passes via text message or verification codes for logging into sites, social media apps publish photos and personal data, fitness and health apps track steps, heartrate, and food intake—a cybercriminal can learn all there is to know about their targets by breaching their cell phone.

Your phone may contain and transmit a larger volume of and more sensitive info than your computers—but it's not always as protected.

Security issues with phones

A number of factors contribute to weak mobile phone security, but one of the top concerns is that phones are much easier to be misplaced, lost, and stolen. Mobile phones go with you everywhere, which means there's more potential for leaving them behind. Once a criminal has physical control over your phone, it's often not too difficult to gain control of its data.

A second huge concern for mobile phone security is the validity of third-party apps. They aren't vetted by the major app stores iTunes and Google Play, therefore they needn't pass a minimum standard for safety. Apple iPhone has strict laws about apps: They can only be downloaded from iTunes, therefore they're more secure. The downside is that users are restricted from going outside the iTunes ecosystem, which is why people sometimes jailbreak their phones. This is a dangerous measure, as it negates all security, not only for apps, but also for operating systems.

Google's Android, however, allows for third-party apps to be downloaded. "Android is highly customizable and open to innovation by its users," says Collier. "Also, although Google highly recommends you only install from the Google Play store, they allow you to take the risk into your own hands if you really want to install elsewhere."

Another security risk with mobile phones is that users don't update their OSes as often as computers. Updating phone software requires ample memory and battery power, and users are often running low on both. Every time a software update is delayed on a mobile phone, a cybercriminal has an opportunity to exploit security vulnerabilities in the operating system.

Of course, mobile phones are also vulnerable to the same pitfalls that befall desktops and laptops—mainly, users who don't practice safe surfing. Social engineering in the form of social media scams and phishing can especially ensnare mobile users who regularly check their email, Facebook, Twitter, and other social networking sites. Phishing in the form of text messaging, or smishing, has also become a popular attack vector, particularly for criminals looking to cash in on the popularity of mobile banking.

Finally, all of these risks are compounded by the fact that technical security measures are not commonplace in phones. While computers are often equipped with firewalls, antivirus, and/or anti-malware software, mobile devices typically have only their operating systems and the security of their apps to protect them.

Ways to stay secure

So what does this mean for mobile phone users? It means that it's even more important to stay vigilant about cybersecurity when using a mobile device. Here are some ways you can protect yourself, your data, and your phone.

1. Lock your phone with a password or fingerprint detection. At the very least, if you leave your phone on the counter at Starbucks or if it's stolen out of your pocket, cybercriminals will have to get through that first gate. Set the time on your password lock to be short as well—30 seconds or less should cut it.
2. If it's not already the default on your phone, consider encrypting your data. Doing so is especially useful for protecting sensitive data, whether that's business emails or investing and banking apps.
3. Set up remote wipe. If your phone is lost or stolen, you'll be able to wipe all of its data remotely (and therefore keep it out of the hands of criminals). You can often also use remote wipe to find your phone's location.
4. Back up phone data. Consider connecting your device to its associated cloud service in order to automatically back up data (and encrypt it). However, if you don't trust the cloud, be sure you connect to a PC or Mac to sync data regularly in order to preserve photos, videos, apps, and other files.
5. Avoid third-party apps. If you're on an iPhone, you don't have much of a choice. However, for Android users, staying on Google Play and not allowing apps from unknown sources keeps you relatively safe. If you *do* decide to use third-party

apps, research to be sure you're not getting a malicious one. Read reviews, and if the app asks for access to too much personal data up front, don't download it.

6. Avoid jailbreaking your iPhone or rooting your Android. While the processes are different, the end result is bypassing what phone manufacturers intended (including security protocols) and ultimately weakening the security of your device.
7. Update operating systems often. When that pop-up reminder comes up, don't ignore it. Charge your phone, clear out some space, and install the update right away.
8. Be wary of social engineering scams. Cybercriminals love to spoof banking apps, send phony texts meant to collect personal data, and email malicious links and attachments. Just as you do on your computer, view any communications from unknown sources with a careful eye. If it seems fishy, it very likely is.
9. Use public wifi carefully. Yes, you don't want to use up all your data. However, public wifi is inherently insecure, so try not to make transactions or transmit sensitive data while using it. Consider using a VPN service to encrypt data transmitted online.
10. Download anti-malware for your mobile device. If you do happen to download a malicious app or open a malicious attachment, mobile anti-malware protection can prevent the infection.

Chances are, you use your phone to do a lot of stuff online. You may even be reading this article on it right now. For peace of mind, and to get a leg up against a rising tide of mobile malware activity, don't just phone it in—be proactive about your mobile security.

https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/?utm_source=double-opt- in&utm_medium=email-internal-b2c&utm_campaign=EM-September-2016newsletter&utm_content=secure-mobile

© 2024 Available Technology Inc