PHYS.ORG

Your smartphone is a target, so make it secure

May 22 2015, by Troy Wolverton, San Jose Mercury News

Credit: Peter Griffin/Public Domain

Consumers beware: Your smartphone represents a uniquely valuable and vulnerable target for hackers, scam artists and other bad actors.

But don't panic. While the security threats to your smartphone are real and growing, they're nowhere near crisis levels. And you can protect your device and your data from many of the biggest security threats fairly easily.

"Remember, this is a computer in your pocket," said Cooper Quintin, a staff technologist at the Electronic Frontier Foundation, a civil liberties nonprofit. "Treat it as such - Use the common sense security practices that you would use on your computer."

Like your wallet, your smartphone carries your personal information and oftentimes stores your bank account and credit card numbers. Smartphones have similar processing power to PCs and similar potential vulnerabilities, but unlike many computers, smartphones have an always-on connection to the Internet.

With the number of smartphones in use rivaling PCs, they have become an increasingly tempting target for bad guys who are catching on to their worth. Some 3.1 million smartphones were stolen in 2013, nearly double the number from 2012, according to Consumer Reports.

The amount of malicious software, known as malware, targeted at devices running Android - by far the most popular smartphone operating system worldwide - is growing rapidly. So too is the amount of so-called adware, code that typically displays what appear to be system alerts, but are actually advertisements that urge consumers to download software.

"It's getting worse and worse, to be honest," said Peter Stelzhammer, who works with AV-Comparatives, a firm that reviews and rates anti-malware products.

And it's not just the hackers and criminals who pose a security threat to users. Even legitimate apps collect plenty of personal data on users and frequently demand access to lots more information and sensors than they really need. App makers can use that data for marketing purposes and share it widely without consumers even realizing what they've collected.

Smartphones also tend to have a whole lot more sensors than PCs, which can be used to track your location and activities and even listen in on your conversations.

Meanwhile, documents leaked by Edward Snowden indicate that the National Security Agency is able to tap into some of the data transmitted by smartphones to cloud-based computers and can secretly use smartphones to spy on their users.

"The cell phone is the most effective surveillance device out there," said Bruce Schneier, chief technology officer at Resilient Systems, an Internet security firm.

You may not be able to completely protect yourself from the NSA or from tracking by legitimate apps, but you can take steps to make your smartphone more secure.

Prevent unauthorized access to your phone if it's lost or stolen by establishing a passcode. On an iPhone, activating a passcode has a second benefit: It serves as a lock for the device's encryption feature, which by default scrambles all the data on it. On Android devices, you frequently have to turn on encryption separately.

Both iPhones and devices running Android now come with software preinstalled and turned on by default that allows you to find them if they are lost and remotely delete personal data from them if they are stolen. Make sure to activate the feature when you set up your phone.

You can avoid the vast majority of smartphone malware by sticking to the official app stores. Most of the bad apps out in the wild are being listed on third-party stores, mostly in places like China and Russia. Apple closely scrutinizes all iPhone apps for security and other issues before they are listed in its store. While the Google Play store is more open, Google also is reviewing the apps within it fairly closely.

Anti-virus programs, which you can run on Android devices but not iPhones, may not be necessary, but they won't hurt to have in place, security researchers say.

You can also limit how much data you share with apps. That's relatively easy on the iPhone, where apps have to ask for permission the first time they attempt to access the camera or contact lists. It's more difficult on Android, where users typically only have one chance to say no to granting access to such data and features - when they install the app. Still, security researchers recommend that consumers look closely at what permissions apps are asking for - and avoid apps that ask for too much.

"If you're installing a game, it shouldn't have access to everything that's on your phone," said Ragib Hasan, assistant professor in the University of Alabama Birmingham's computer and information science department. "If there's something fishy, you should not install it."

Beyond that, take some of the same precautions you would take on a PC. Think before you click on emailed links or attachments, and be careful what sites you visit.

"Common sense is always the best line of defense," the EFF's Quintin said.

—-

PROTECTING YOUR PHONE

Security threats to your smartphone are proliferating. Here are six ways to protect your device and data.

-Use a passcode: A PIN or password can prevent others from unlocking your device.

-Use encryption: Encryption scrambles phone data so it can't be read by unauthorized users. iPhones encrypt data by default when you turn on a passcode. On Android devices, you often have to turn on encryption separately.

-Scrutinize permission requests: Many apps, particularly on Android, ask for more permissions than they necessarily need. On iPhones, you can block apps' access to particular features or data. On Android, you may have to simply avoid certain apps.

-Stick to official app stores: Most smartphone malware is being distributed through third-party app stores, typically in places like Russia and China. Apple and Google, by contrast, have done a good job of keeping bad apps out of their stores.

-Use 'find my phone' features: Apple's Find My iPhone and Google's Android Device Manager help users locate lost phones and allow them to delete data from stolen ones.

-Run anti-virus software: You can't run anti-virus programs on iPhones, but you can on Android devices, often for free. The best ones will catch as much as 99 percent of known smartphone malware.

©2015 San Jose Mercury News
Distributed by Tribune Content Agency, LLC.

Citation: Your smartphone is a target, so make it secure (2015, May 22) retrieved 20 April 2024 from https://phys.org/news/2015-05-smartphone.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.