PHYS.ORG

Go-everywhere, do-everything phones usher in host of security concerns

March 10 2011, By Victor Godinez

Chances are you lock your door when you leave home, don't leave the keys in the ignition when you run into the 7-Eleven for milk and have at least some kind of security software on your computer. But what about your smart phone?

For many people, a phone these days is a mobile office crammed with valuable contacts, a digital wallet from which you buy songs on iTunes or shoes on Amazon, and a portal to your online bank account.

Rather than locking the phones like bank vaults, most smart phone owners treat their devices with as much concern as they do Monopoly money.

According to a survey by data security provider Symantec, 54 percent of smart phone users do not have a password lock on their phones when they turn them on or wake them from sleep mode.

"I think there's definitely an awareness gap right now," said Mark Kanok, group product manager for the Norton mobile division at Symantec.

"Just a few years ago, your phone was a phone. Then the iPhone comes out and people are downloading apps. People are now starting to ask the questions about, 'How is this going to affect my privacy, what happens if I lose it,' things like that."

On top of the dangers of your phone being lost or stolen, there are also a growing number of malicious apps designed to steal data from it or rack up huge texting bills.

Last week, Google pulled several dozen free apps from its Android market that had been stuffed with damaging code.

Symantec estimated that the apps were downloaded anywhere from 50,000 to 200,000 times in a four-day period before they were pulled.

John Thode, vice president and general manager of the mobility product group for Dell Inc., said many smart phone users don't realize the value of their device until it's gone.

"The reality is that, yeah, whenever you lose your phone or your phone breaks, there's an instant panic that comes around," he said. "Holy smokes, where are my contacts? How do I get back my whole life?"

That concern is magnified when an employer starts giving out smart phones to its workers or lets those workers connect their personal devices to the corporate network, said Mary Chan, vice president of Dell's enterprise mobile solutions division.

Chan's group has begun offering security systems and procedures for mobile devices on corporate networks.

She said a compromised phone with access to a corporate network can wreak havoc.

"I think most of the IT and CIO folks are really concerned about managing the device itself, managing what's being loaded on the device," she said.

Chan pointed to an estimate by research firm Gartner that roughly 300 million smart phones will be connected to corporate networks by 2015, with about half those devices being employees' personal machines.

Much of the security advice for individual smart phone users and corporate managers overlaps.

Only install trusted apps on your phone.

Use Web-based programs that let you remotely track or delete all of the data on your smart phone if it gets lost.

Don't conduct financial transactions over public or unfamiliar Wi-Fi networks, where your data can flow through a hacker's router.

Employers can also take additional steps, Chan said, such as letting employees only install apps from a pre-approved list.

Another option is keeping valuable corporate data only accessible online, rather than letting individual users download it to their phones.

Phone makers and software developers are pushing out some of these tools to smart phone users.

Apple, for example, offers free software on the iPhone and iPad that lets users remotely set up a password lock if the device gets lost or stolen, track it geographically or even wipe all the data from the machine as a last resort.

Norton Mobile Security for Android devices includes a malware scanner that is designed to catch crooked apps before they bite you.

Even with technological protection, user awareness can go a long way.

Simple games and screen saver apps, for example, shouldn't be asking for permission to access your text messages. If they do, you're probably better off canceling the installation.

Strong security software and individual vigilance will become even more important over the next few years as phone makers and carriers adopt a technology that will turn your phone into a wireless digital wallet.

So-called near-field communication, or NFC, systems should make life more convenient, letting you store your credit and debit cards and, eventually, your driver's license digitally on your phone.

You'll simply wave your phone over a scanner at the cash register to pay and be on your way.

But as our phones become more valuable to us, they'll also become a more tempting target for thieves.

"Once NFC starts happening, you're going to see hackers enter this space in a much more substantial way," said Thode at Dell.

Apple is rumored to be including an NFC chip in the next-generation iPhone expected this summer, and Samsung has already released the NFC-equipped Nexus S.

Kanok at Norton said the growing need for better smart phone security seems to be sinking in.

"I think the maturity is a little bit lagging behind where we are on the PC front," he said. "But I think the sensitivity has picked up over the last year."

Distributed by McClatchy-Tribune Information Services.

Citation: Go-everywhere, do-everything phones usher in host of security concerns (2011, March 10) retrieved 23 April 2024 from https://phys.org/news/2011-03-go-everywhere-do-everything-usher-host.html