

Experts: Smartphones another avenue for hackers

TONY WINTON, Associated Press

MIAMI (AP) -- Smartphones are increasingly popular not only with consumers, but also with thieves who see the devices as another way to tap into bank accounts and other sensitive information, experts say.

Many consumers simply don't realize how vulnerable their Androids, iPhones and other devices can be. An April study by the Federal Reserve Bank of Atlanta said threats are proliferating, ranging from "phishing" - where consumers click a phony email or text message and are tricked into handing over personal information - to consumers' reluctance to use security protections they normally have on home computers, like a password.

The study said there are several things that can make smartphones an easy target. Vast amounts of personal data are stored in emails, texts and other applications, and personal information is increasingly easily found on social media. Organized crime operations also see smartphones as the most vulnerable entry point into the electronic financial system, according to the Federal Reserve.

"We have some very bad characters who would like to take our money, take our identification, and run away with it," said Marie Gooding, first vice president of the Atlanta Fed.

Research the Fed cited, done by Boston-based Trusteer Inc., involved 20 computer servers that were used to send out more than 100,000 "phishing" emails. By studying the server records, Trusteer found that about 2,200 of the 3,000 responses the scam artists received came from smartphones.

Doug Johnson, vice president of risk management for the American Bankers Association, said he expects those numbers to get worse.

"This is one more platform criminals will continue to exploit as the channel grows," he said.

The Fed helps operate the industry's Automated Clearing House, a system that processed 21 billion transactions last year. While banks are required to adhere to authentication standards for ACH transactions, those protections are often unknowingly compromised by consumers.

"A lot of it has to do with all of the players making sure they have the strongest security controls they have, and then consumers being aware of what those controls are, and making use of them," Gooding said.

Experts: Smartphones another avenue for hackers

Published on Electronic Component News (<http://www.ecnmag.com>)

Miami attorney Andrew Carter learned the hard way, after misplacing his phone amid the hubbub of a Christmas vacation. He had a mobile banking app installed on his phone, but had turned off his passcode lock because he found it annoying to enter whenever he wanted to use the phone.

"That was a big mistake," he said. "I knew it intellectually, but I hadn't really intuitively grasped that I had to be able to be a lot more secure with it."

Weeks later, Carter found \$2,000 had been withdrawn from his account by someone in Texas, possibly through emails retrieved from his phone. He also found someone trying to hack his Facebook account.

Today, he keeps his phone locked and changed to a brand that allows him to remotely erase phone data - something he couldn't do with his old phone.

Several manufacturers are planning new "biometric" technology, such as fingerprint scanners, that can make phones more secure. But even with those safeguards, consumer behavior can still lead to danger.

Vikram Thakur, principal security response manager for security software giant Symantec, said attackers can get complete control of a phone simply by getting people to click on a link. Without actually having the phone in their hands, the hackers can access messages, phone calls and personal information.

"The amount of information we're storing on mobile phones these days kind of incentivizes the attackers to go after the platform," he said.

Source URL (retrieved on 04/23/2014 - 10:15pm):

<http://www.ecnmag.com/news/2013/05/experts-smartphones-another-avenue-hackers>