As mobile payments field grows, so do security concerns

April 11 2013, by Kirk Ladendorf

Mobile payments technology, over time, could have a profound impact on the way products are sold, bills are paid and money is transferred around the world.

But some of the experts who look at the new technology say they have unanswered questions about the security and privacy issues tied to the payments format.

Payments industry executives say the technology is good and getting better. But security experts say the swift growth of smartphone use inevitably is going to attract fraud. And as more consumers use their mobile phones as payment devices, the potential risks can increase.

Dallas-based NQ Mobile, which provides security software for smartphones, says it saw more than 65,000 new malware threats released worldwide in 2012, up from 24,000 the year before. Malware and phony app sites can direct unsuspecting phone users to sites where they give up sensitive personal information, such as bank account passwords.

"It is a real problem, and it is growing," said Gavin Kim, chief commercial officer of the company. "Smartphone sales are booming, and they are becoming a much more targeted device by hackers." The company sells software that can identify mobile phone apps sites and protect users against malware and viruses.

Interest in the mobile phone security software is growing, but the

company estimates that only about 8 percent of the mobile market actually uses security products on phones.

Executives in the payments industry say payments processors and their network of affiliated merchants are constantly improving technology and processes to combat fraud.

"I am completely comfortable and confident in the level of security of these transactions. In our system, the information is encrypted from end to end," said Brent Warrington, CEO of Austin, Texas-based SecureNet, which processes both online and mobile payment transactions.

While security concerns are being addressed rapidly, privacy advocates see no quick remedy for concerns about potential misuse of growing mountains of electronic data tied to the spending patterns of individual consumers.

The same technology that makes mobile payments convenient also makes it easier for data analytics companies to get a better fix on where they spend their time and where and what they buy. Data analytics companies already pore through massive amounts of consumer data in order to give retailers and lenders a better idea of how to market to them.

Some of those tech analytics companies compile secret "e-scores" that rank consumers and that are claimed to predict consumer spending. That trend alarms some privacy advocates, such as Jeff Chester with the Center for Digital Democracy in Washington. Chester says mobile payments can create another deluge of data that enable some clever analytics companies to score and secretly rank them as consumers.

Mobile payment "is about exposing your financial behavior to a daisy chain of financial and other marketers who have a very detailed

understanding of where you are, how you spend your time and what you buy," Chester said in an interview with McClatchy Newspapers.

Personal health information and credit scores are closely guarded information in this country. Chester believes other data that go into e-scores also should be regulated to prevent invasion of privacy and unfair discrimination by retailers and other businesses.

At present, he said, there are no such protections to the new kinds of data, which will proliferate with mobile payments.

The collection of data, Chester said, "needs to be transparent and accountable. All these new, nontraditional data services are unregulated, and they need to be regulated. There should not be any kind of financial profile on a consumer that he or she can't have access to to review and to challenge."

SECURITY TIPS

Mobile payments security tips from NQ Mobile include:

-"Locking" the phone with a password to protect stored data if the phone is stolen or lost.

-Installing security software on the phone.

-Keeping the phone clean of personal data such as address information and bank account information.

-Being very careful not to provide personal information when downloading new apps from unknown sources.

-Being wary of using personal information when connected to the

Internet over public Wi-Fi hotspots.

-Notifying the mobile carrier quickly when the phone is stolen so it can disable both the phone and the apps that are on it.

(c)2013 Austin American-Statesman, Texas
Distributed by MCT Information Services

Citation: As mobile payments field grows, so do security concerns (2013, April 11) retrieved 27 April 2024 from https://phys.org/news/2013-04-mobile-payments-field.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.