

MORE TO WORRY ABOUT: Beware the apps

By John Ginovsky

With the onslaught of electronic channels— from online and mobile banking to social media marketing— and the proliferation of gadgets— smart phones, tablets, and ever-slimmer laptops— the opportunity for cyber threats is increasing exponentially.

Some analysts see an emerging vulnerability in the applications (apps) downloaded in this mobile, digital world. Although there doesn't seem to be any statistical analysis of this threat— yet— the potential is reasonable.

In particular, two areas may be prone to do damage: malware installed on apps and fake apps that could entice users to provide confidential information.

Regarding the former, "When you go to your app store and download a free app, no one really knows what's inside it, outside the person who wrote it," says Michael Urban, Fiserv's director of financial crimes risk management. Even the purported app writer may not fully understand what's included, he explained to Tech Topics. Why? The writer may hire others to write discrete pieces of code.

"It's very difficult to understand if there is something inside this app that's going to do something, at some point of time, that you don't want to happen," Urban continues. "It could install malware, it could get some information, and it could send it off somewhere. There isn't really that level of analysis and vetting done on the apps that are provided for sale, let alone the apps that you can find on the internet."

Even fake bank apps made a brief appearance, Urban says. "There were a couple of Android market apps that used legitimate bank logos. The idea was to get you to install the app, and then ask you to provide your credentials. Then it stripped the credentials and didn't really work," he says. Urban points out that these apps were removed from the app store, "but it just shows that many times, with the amount of vetting that's going on out there, those apps aren't always checked."

Any advice? "Make sure that you've got a process in place that's monitoring app stores and the

internet generally," Urban says. Banks already may do this from a branding perspective to protect themselves against phishing sites or tweets about bad experiences, for example. But such web-presence monitoring "needs to be extended into app stores as well," he explains, "so that if there is something that comes in there that's using your brand, you want to be able to know as quickly as possible and understand what steps to take, whom you would contact, in order to manage that type of situation."

At the same time, Urban says, as a bank builds its own legitimate mobile app, appropriate precautions need to be taken. "It's just as important to protect and have secure coding practices in mobile as it is anywhere else in the institution."

About the Author

John Ginovsky is contributing editor of ABA Banking Journal and editor of the publication's TechTopics e-newsletter.

For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News. You can email him at jginovsky@sbpub.com

[This article was posted on May 15, 2012, on the website of ABA Banking Journal, www.ababj.com.]