Badger Bank
Working Together, Achieving Success.

Badger Bank

Monthly Security Tips
NEWSLETTER

June 2014

Protecting Against Mobile Malware

From the Desk of Steve Dehnert, Badger Bank President & CEO

Is Malware a Threat to Mobile Devices?

The volume of cyber threats to mobile computing devices continues to increase as new applications (apps) and devices proliferate.

McAfee® reports that there were more than two million new mobile malware samples in 2013. Symantec™ reports that nearly 40 percent of mobile device users have experienced mobile cybercrime in the past 12 months. Some experts estimate that nearly 10 percent of applications sold on particular platforms are malicious.

Most mobile malware gets installed when a user visits an infected website, downloads a malicious application or clicks on a link or an attachment. Some of the threats to mobile devices include the following:

- Theft of personal data, such as account info, telephone numbers, contact lists, call logs, etc.
- Propagation of malware to your contacts by posting to social media, sending phishing emails, etc.
- Surveillance through audio, video (camera), location, text messages, telephone calls and other means
- Disabling of monitoring software on the mobile device
- Collection of data, such as GPS readings, to track a user

What Can I Do to Secure My Mobile Device?

The following are examples of how you can secure your mobile device:

- **Lock the device** — An easy way for malware to get on a device is for someone to manually install it. Locking your device with a strong PIN/password makes unauthorized installation of apps more difficult.
- **Install apps from trusted sources** — Users must recognize that some apps may be malicious. If an app is requesting more permissions than seems necessary, do not install it, or uninstall the app. Only install apps from trusted sources.
- **Don't jailbreak your device** — To "jailbreak" or to "root" a device means to bypass important controls and gain full access to the operating system. Doing this will usually void the warranty and can create security risks. This also enables apps, including malicious ones, to bypass controls and access the data owned by other apps.

- **Keep operating systems and apps up to date** — Manufacturers, telecommunications providers and software providers regularly update their software to fix vulnerabilities. Make sure your device's operating system and apps are regularly updated and running the most recent versions.
- **Use a mobile security software solution** — Install anti-virus software, if available.
- **Block Web ads or don't click on them** — Malware can find its way onto your mobile device through a variety of methods, including advertisements (ads). The malicious ads are called "malvertisements." Mobile ads accompany a significant amount of content found in mobile apps, and whether you find them annoying or amusing, cybercriminals have turned their attention toward using them to spread malware to unsuspecting users. What makes these "malvertisements" so dangerous is the fact that they are often delivered through legitimate ad networks and may not appear as outright spam but can contain Trojans or lead to malicious websites when clicked on. Some mobile devices have software that can block harmful sites.
- **Don't click suspicious links and attachments** — While it may be difficult to spot some phishing attempts, it's important to be cautious about all communications you receive, including those purported to be from trusted entities. Also, be careful when clicking on links or attachments contained within those messages.
- **Disable unwanted services/calling** — Capabilities, such as Bluetooth® and near field communication (NFC), can provide ease and convenience in using your smartphone. They can also provide an easy way for a nearby, unauthorized user to gain access to your data. Turn these features off when they are not required.
- **Don't use public Wi-Fi** — Many smartphone users take advantage of free Wi-Fi hotspots to access data (and keep their phone plan costs down). Smartphones are susceptible to malware and hacking when leveraging unsecured public networks. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.