April 2015
Volume 10, Issue 4

Security in the Mobile Era

Clark County Information Technology

From the Desk of Louis Carr, Jr., Chief Information Officer

By 2017, the number of smartphone users in the U.S. is expected to surpass 200 million, nearly 65 percent of the population.[1] Negotiating security in the face of an ever-growing implementation of mobile devices presents serious challenges for organizations. Risks include the growth of Bring Your Own Device (BYOD) (coupled with a lack of security controls for these devices), loss/theft of devices, and the proliferation of mobile malware.

Users need to understand the risks and the steps they can take to minimize them, particularly as cybercriminals often use employees as the entry point into an organization's network. Below are some key actions users can take to help minimize the likelihood of a successful cyber attack.

Regularly update your device.
Mobile malware increased 75% in 2014 from 2013[2], and further increases in malware are expected in 2015, particularly in mobile ransomware. Updated operating systems and security software are critical in protecting against emerging threats.

Enable encryption.
Enabling encryption on your smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.

Use a passcode.
In case your phone ever does fall into the wrong hands, don't make it easy for someone to access all your important information! Enable strong password protection on your device and include a timeout requiring authentication after a period of inactivity. Secure the smartphone with a *unique* password - not the default one it came with. Do not share your password with others.

Do not use public Wi-Fi.
Do not log into accounts and do not conduct any sensitive transactions, such as shopping or banking, while using public Wi-Fi. Disable the "automatically connect to Wi-Fi" setting on your device.

Install applications from trusted sources.
Last fall, Gartner issued a prediction that more than 75 percent of mobile applications will fail basic security tests through 2015.[3] When downloading apps, be proactive and

[1] http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694
[2] http://www.cnbc.com/id/102338872

make sure that you read the privacy statement, review permissions, check the app reviews and look online to see if any security company has identified the app as malicious.

Install a phone locator/remote erase app.
Misplacing your device doesn't have to be a catastrophe if it has a locater app. Many such apps allow you to log on to another computer and see on a map exactly where the device is. Remote erase apps allow you to remotely wipe data from your device, helping minimize unauthorized access to your information in the event you cannot locate the device.

Disable unwanted services when not in use.
Bluetooth and Near Field Capabilities (NFC) can provide an easy way for an unauthorized user near by to gain access to your data. Turn these features off when they are not required.

Carefully dispose of mobile devices.
With the constant changes in the smartphone market, many users frequently upgrade to new devices. Make sure you wipe the information from your smartphone before disposal. For information on how to do this, check the website of your mobile provider or the manufacturer.

Provided By:

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.

---

[3] http://www.gartner.com/newsroom/id/2846017