

Protecting Against Mobile Malware



From the Desk of the Enterprise Information Security Administrator, ND ITD

Is Malware a Threat to Mobile Devices?

The volume of cyber threats to mobile computing devices continues to increase as new applications and devices proliferate. McAfee reports that there were more than two million new mobile malware samples in 2013. Symantec reports that nearly 40% of mobile device users have experienced mobile cyber crime in the past 12 months. Some experts estimate that nearly 10% of applications sold on particular platforms are malicious.

Most mobile malware gets installed when a user visits an infected web site or 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, phone numbers, contact lists, call logs, etc.
- Propagation of malware to your contacts either through by posting to social media, sending phishing emails, etc.
- Surveillance through audio, video (camera), location, text messages, phone 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?

1. 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 applications more difficult.

- a. **The North Dakota Enterprise Architecture Mobile Device Access Control Standard ST013-07.1** states,
 - i. “A power-on password shall be used and shall at least be a 4-digit number.”
 - ii. “Automatic device locking shall occur after five (5) minutes of inactivity.”
 - iii. “When configurable, devices shall be disabled after ten (10) successive invalid sign on attempts. If a device becomes disabled, this means the device has all of its local information erased and it must be reconfigured to connect to the State’s servers.”

2. Install applications from trusted sources

Users must recognize that some applications may be malicious. If an app is requesting more permissions than seems necessary, do not install it, or uninstall the application. Only install applications from trusted sources.

3. 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 applications, including malicious ones, to bypass controls and access the data owned by other apps.

4. 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.

5. Use a mobile security software solution

Install antivirus software, if available.

6. Block web ads or and don't click on them

Malware can find its way onto your mobile device through a variety of methods, including advertisements. The malicious advertisements are called "malvertisements." Mobile ads accompany a significant amount of content found in mobile applications, and whether you find them annoying or amusing, cyber criminals 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 outright spam, but can contain Trojans or lead to malicious websites when clicked on. Some mobile devices have software that can block harmful sites.

7. Don't clicking 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" and be careful when clicking on links or attachments contained within those messages.

8. Disable unwanted services/calling

Capabilities such as Bluetooth and 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.

9. Don't use public Wi-Fi

Many smartphone users use 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.

For More Information

What is the North Dakota Enterprise Architecture Standard on Mobile Device Access Control?

<http://www.nd.gov/itd/standards/security/mobile-device-access-control>

What is a computer virus?

<http://www.microsoft.com/security/pc-security/virus-what-is.aspx>

When Malware Goes Mobile

<http://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/business-of-cybercrime.aspx>

10 Years of Mobile Malware: How Secure Are You?

<http://www.linkedin.com/today/post/article/20140316112657-67886711-10-years-of-mobile-malware-how-secure-are-you>

Mobile Threat Report: 2013 Q3

[http://www.f-secure.com/static/doc/labs_global/Research/Mobile Threat Report Q3 2013.pdf](http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q3%202013.pdf)

Mobile Malware Evolution: 2013

[https://www.securelist.com/en/analysis/204792326/Mobile Malware Evolution 2013#08](https://www.securelist.com/en/analysis/204792326/Mobile_Malware_Evolution_2013#08)

Mobile Threat Report

http://www.webroot.com/shared/pdf/WR_MobileThreatReport_v4_20140218101834_565288.pdf

Fake Android Apps

<http://us.norton.com/fake-android-apps/article>

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 ND Information Technology Department 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.