



Tech Insight: Mobile Security

Volume 6, Issue 4

Office of Information and Technology (OIT)

Mobile security refers to the [protection of mobile devices](#), such as smartphones, laptops, and tablets, and their *connected networks*, from threats and vulnerabilities associated with wireless computing. Since the time of the world's first mobile phone call in April 1973, when a senior engineer at Motorola called a rival telecommunications company to inform them that he was speaking via a mobile phone; to the commercialization of the Internet in 1994, [mobile security](#) has become an increasingly significant concern to government, education, and industry. But perhaps the greatest cultural paradigm shift to impact wireless computing has occurred only recently as more office workers than ever are successfully conducting business remotely, a work style that permits professionals to work outside a traditional office environment.

Mainstream America uses mobile devices to connect to more wireless networks in places that may implement little or no network security measures (i.e. hotels, coffee shops, and airports), as they use their own personal devices to tether onto cellular networks. Data leakage is now a significant risk for mobile security. This Tech Insight, a continuation of [Tech Insights: Mobile Security \(January 2016\)](#), will highlight new mobile security concerns and enterprise solutions, including tips on how to secure and protect devices and networks.

Overview

The use of smartphones by American adults to conduct public, private, and government business has risen to [77 percent from 64 percent](#) in just the last three years. As of February 2018, the use of tablets has risen to 53 percent while the use of laptops has declined. Thus, the data suggests that technology users are becoming increasingly mobile, as smaller mobile devices are now able to perform similarly to laptops and desktop computers. Concurrently, mobile devices have become a repository of sensitive data that includes protected health information (PHI) and personally identifiable information (PII), creating an even greater need for mobile security.

Mobile devices are equipped with wireless technologies, such as wireless network adapters, Bluetooth, Short Message Service (SMS), Multimedia Messaging Service (MMS), Near Field Communication (NFC), and Global System for Mobile Communications (GSM). SMS and MMS are both texting technologies, while GSM is the mobile data network that is commonly referred to as 2G (Second Generation), with newer generations that include 3G and 4G. NFC is used to create a connection when two devices are within very close range or touching each other. In addition, smartphones, tablets, and laptops use applications that permit pervasive access to networks, with the ability to collect their own data, as network access parameters are controlled by the user. With so many avenues for connecting, is it any wonder that mobile devices have become exploited targets?

Attack Targets

As listed in [Tech Insight: Mobile Security \(January 2016\)](#), data, identity, and availability are still prime targets of attack for hackers. A hacker can limit the *availability* of the user's own access to personal *data*, including highly sensitive proprietary data, gaining access to the user's identity.

Security Threats, Vulnerabilities, and Risks

[Security threats, vulnerabilities, and risks](#) are terms that are used interchangeably, but have different meanings and implications. Threat refers to a new or newly discovered incident with the potential to do harm to a system or organization. Vulnerability refers to a known weakness of an asset that can be exploited by one or more attackers. Risk refers to the potential for loss or damage when a threat exploits a vulnerability. Loss or theft of a device; malware (malicious software); and data leakage, the unauthorized transmission of data from within an organization to an external destination; are a few examples of threats, vulnerabilities, and risks. The following represent examples that are making their way to the [top of the list of concerns](#):

1. **Out-of-date operating systems and applications:** Users don't always update the device operating system (OS) or applications when security and other patches for are released. Users sometimes fear how the device will operate after installation or they are concerned about the availability of space consumed by the new release. When the user fails to update the device with new software releases, the existing code is vulnerable.
2. **Unsafe connections:** Users often work remotely, requiring them to use wireless fidelity (Wi-Fi) connections that may not be secure, or they may use their mobile networks without password protection or encryption. These connections leave devices vulnerable to attack from multiple sources.
3. **Uncontrollable users:** These are users who do not always follow the rules for reducing risks when it comes to safe device usage.
4. **Lack of device monitoring:** In organizations that have many employees, it is difficult to monitor all devices that are in use. Each device may hold numerous applications, increasing the difficulty to monitor network usage.
5. **Device variety:** Most organizations don't have a single purchasing contract with a single device manufacturer. This leads to the use of many different operating systems and

applications. This causes problems with device and application management in the organization.

Solutions to Mobile Security Concerns

Every organization has the challenge of finding a solution to mobile security. Although there is no “cure all” for threats, vulnerabilities, and risks, there are several combinations of solutions that can mitigate potential issues.

Our [previous Mobile Security Tech Insight](#) highlighted the importance of Enterprise Mobility Management (EMM), which is a combination strategy of three management processes. Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Information Management (MIM) all seek to mitigate threats, vulnerabilities, and risks that come from the devices, applications, and networks that may transmit sensitive data. Another important factor is the human element. User education and compliance plays a big role in mitigating threats, vulnerabilities, and risks.

The ways to mitigate the cost of device exploitation are to:

- Set an OS and application update schedule that is outside of peak usage. Setting an update and restart schedule at 2 a.m. on a workday helps devices run smoothly and keeps their security updates current.
- Ensure that network connections are secure. A shared network in a coffee shop, airport, or hotel is public and passwords are not protected. The use of a [Virtual Private Network \(VPN\)](#) application ensures that users are safe on a public network. When PHI/PII is being viewed, saved, and transmitted, encryption standards should be employed.
- Provide user device education. Most organizations have device usage policies in place to ensure users aren't the cause of the issue. User education is paramount to mitigating risks associated with misuse.
- Ensure that the organization selects device manufacturers that reduce costs in device purchasing and reduce any confusion in MDM procedures.

Mobile Security at VA

Mobile users at VA include Veterans, caregivers, providers, VA staff, and external partners. Since mobile solutions at VA are aimed at improving the health of Veterans, security is at the forefront of the VA response in publishing the *Mobile Device Security Policy* [VA Handbook 6500.10](#) on February 15, 2018. The new policy advocates for centrally managing and securing VA government furnished equipment (GFE) mobile devices (e.g., smartphones and tablets) that are used by VA employees and contractors to access the Department's information resources.

Mobile application security once relied on an internal implementation of an Open Authorization (OAuth) 2.0 Authorization Service. This made integration difficult. Now, VA is using [Identity and Access Management's \(IAM\) standard authentication approaches](#) to authenticate users. You can peruse the IAM Enterprise Design Pattern (EDPs) from the [OIT website](#) to learn more about VA's

unified enterprise IAM program that coordinates secure access to VA resources for both internal and external users. Another way VA is securing mobile data is to implement standards for mobile device usage. All mobile projects leverage the approved tools and technologies listed internally at the [VA Technical Reference Model \(TRM\)](#). (External vendors may utilize a less comprehensive [TRM site](#) on the web).

Mobile technologies used by VA stakeholders, such as the Health Records on iPhone app and others offered through the VA App Store, help them manage healthcare needs on-the-go. Applications can be installed on Android, Windows, and Apple devices. This means PHI/PII is no longer stored behind a counter, but in the stakeholder's pocket, backpack, or car. It increases the need for data to be secured from threats, vulnerabilities, and risks.

Conclusion

Mobile security is an ever-evolving issue that organizations and users battle with every day. Information Technology (IT) departments are better equipped to handle the day-to-day operations with the deployment of an EMM. Individual users must also take the time to ensure they are properly defended against data loss due to threats, vulnerabilities, and/or risks. This is where user education falls into the mix. With proper education, users will know how and when to install updates, ensure a network is secure, connect to a secure network, and use devices that are secure.

For more information on user education, the following website is a useful resource on the use of the internet and mobile devices and is applicable to all ages: [Mobile Device Safety](#). For related mobile security information, read our [Mobile Veteran-Facing Application Security](#) EDP, the [Mobile Architecture](#) EDP, or the [Staff-Facing Devices and Applications Security](#) EDP.

The Tech Insight Series

The monthly Tech Insight series aims to help readers make better decisions and be more informed customers of OIT products and services by providing them with high-level overviews of technologies that impact or will impact VA's IT environment. Tech Insights introduce topics in an easily digestible fashion by presenting background information on the topic, clearly explaining its importance within VA, and providing recommendations for success from OIT. All Tech Insights are available [here](#).

Disclaimer: *This document includes links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.*