10 Mobile Device Threats in Higher Education

and How to Combat Them
Introduction: The State of Mobile Data Risks

Education institutions face numerous data security challenges, including tight budgets, the need for unrestricted connectivity to online learning resources, and increased regulations. To understand the pressing challenges facing these institutions, Dell SecureWorks hosted a series of roundtable events across the U.S. in 2012. Attendees representing a wide spectrum of education institutions shared their perspectives on data security, and discussed the security threats they now confront, as well as the emerging dangers and risks they perceive they will face in the near future.

Several themes emerged, including:

**Policies around mobile device security are generally weak or non-existent.** Formally enforced and managed bring-your-own-device (BYOD) policies, device usage and tracking, data encryption and identity and access management were absent at almost all of the panelists’ institutions.

**Students represent an enormous inside risk.** Although higher education institutions recognized that outside attacks are prevalent threats, risks from students were of equal or greater concern. Specific issues are password sharing, the popularity of reverse engineering, tracking myriad and rogue devices connecting to the network, and the fact that many students are now very tech-savvy.

The trend toward increased connectedness with mobile devices ranging from smartphones to tablets, and BYOD programs is becoming increasingly recognized in the higher education community. In fact, Educause, a leading provider of guidance to education IT professionals, lists “trends toward IT consumerization and BYOD” as one of the top ten issues of 2012 in a recent report.¹ Educause had already noted in a 2011 survey that security and data breaches ranked in the top five IT concerns that higher education institutions face.² According to the report, “hackers [are] repeatedly finding ways to defeat the best technical, organizational, and social countermeasures created by security experts. We are seeing new exploits that automated intrusion detection fails to recognize, malware that is difficult to remove, and whole new waves of risk associated with the rapid deployment of smartphones and the new generation of tablets on institutional networks.”

Although security is on the radar of higher education IT departments, there often isn’t visibility into exactly what the magnitude of the threat really is across the entire spectrum of the institution’s infrastructure. In many organizations, smartphones are replacing or complementing computers, creating new security vulnerabilities. Complicating matters, smartphones run on up to ten mobile operating systems today, with security-related products that offer varying capabilities depending on the device and mobile operating system used. However, several precautions can greatly minimize the risk that mobile devices pose. This whitepaper outlines ten of the most common mobile device threats, along with recommendations to combat them.

---

¹ http://net.educause.edu/ir/library/pdf/ERM1232.pdf
² http://www.educause.edu/ero/article/top-ten-it-issues-2011
Many security breaches occur because users don’t understand the risks associated with everyday actions.

Threats and counter measures

Below are ten of the more common threats associated with smartphones and mobile devices, along with best practices to help mitigate risks.

1) **Wi-Fi Man-in-the-Middle Attacks**: This is a popular and effective means of attack, particularly in coffee shops, bars, restaurants and airports that offer wireless Internet access without requiring a password. In this environment, any hacker on the same network can get into your device in less than five minutes, enabling them to download any unencrypted data, email, contacts, and files. Even without hackers present, laptops, tablets, and smartphones that are infected with malware can search for other vulnerable devices, infect them, and send information back to the hacker.

**Recommendation**: Turn off your Wi-Fi unless you are using a secured campus network or your home network. Use a Mobile VPN product if your institution has one. If you are encrypting your desktop/laptop, include the contents of your smartphone. Unfortunately, most smartphones purchased today have little or no encryption capability.

2) **Bluetooth Man-in-the-Middle Attacks**: Unsecured Bluetooth headsets can provide an easy entry point for hacker to listen to phone conversations, make calls, and download data. Why would you secure the smartphone but leave your Bluetooth headset open?

**Recommendation**: Unless you are using an encrypted Bluetooth headset — and the overwhelming majority are not — turn off Bluetooth and use a wired headset. Again, as a general recommendation, if you are encrypting your desktop or laptop, an encrypted Bluetooth headset is appropriate.

3) **Lack of Awareness and Standardized Policies**: Many security breaches, whether on mobile devices or laptops and desktops, occur because users don’t understand the risks associated with everyday actions.

**Recommendation**: Create and maintain a portable media and device policy to describe expected employee and student behavior. Create an End User Acceptance Policy that contains clear requirements and expectations for mobile devices, including university-owned as well as personal-owned devices that are allowed to access enterprise resources. Educate all users on the content of these policies on a recurring basis, and update each as necessary to respond to the changing mobile device landscape.

4) **Compromised Devices and Open Gateways**: Stolen phones and devices login to networks every day, exposing corporate data to unauthorized disclosure or modification.

**Recommendation**: Use a mobile NAC (Network Access Control) software solution that authenticates, reviews, and compares devices to your policies before allowing them into the collegiate environment. Blocked devices that fail to meet the policy requirements can be quarantined to a site outside the DMZ. IT should require registration of employee- or student-owned devices that will access institutional resources.
5) **Social Media Vulnerabilities**: Advanced and persistent hackers use social sites to collect data about you, your network of colleagues, and friends to create targeted and malicious emails. The personal information posted on these sites is used to help create a relationship of trust, in hopes that you’ll open an email link connected to an infected web site.

**Recommendation**: Limit your employees’ and students’ exposure on social sites by discouraging them from sharing detailed personal data such as their full birthdate, and closely reviewing “friend” requests and emails. Instruct them to never click on links in an email from people they haven’t met personally – and even then, to be wary.

6) **Unprotected Institutional Data**: Do you know what data should be protected and where it is physically located? If not, you’re not alone. Many institutions fail to perform any data classification and location assessments. The importance of data classification and appropriate security controls, like encryption and Data Leak Prevention (DLP) systems cannot be emphasized enough.

**Recommendation**: Perform a DLP storage assessment to understand where your key data and intellectual property sits. Implement controls appropriate to the risk of data loss.

7) **IT Compliance Failures**: Even as more institutional data is stored on personal devices, many organizations have not adequately assessed the risks of allowing personal devices in their environment. Likewise, they fail to understand or implement the appropriate controls to ensure compliance with regulatory and corporate governance requirements.

**Recommendation**: Review the institution’s governance requirements and the organizational risk appetite as part of an overall approach to mobility security. Implement appropriate tools, including mobile device management solutions to deploy and enforce corporate mobile policies. Secure mobile messaging to encrypt corporate email on mobile devices, and secure mobile application development tools, which deliver mobile applications in encrypted containers to prevent unauthorized access. Each of these solutions allow for the remote deletion of corporate information from lost or stolen mobile devices.

8) **Unmanaged Mobile Devices**: Mobile devices left unmanaged by IT expose the environment to excessive risk, including data leakage through connection to unauthorized networks and Bluetooth devices. Lax security controls may allow unauthorized access to institutional information if a device is lost or stolen.

**Recommendation**: Implement a Mobile Device Management solution to provide centralized management and enforcement of corporate policies, password requirements, hardware and device control, certificate management, reporting, and problem alerting.

9) **Smartphone Viruses**: Viruses continue to proliferate via untrustworthy mobile applications, and as many as half of them are undetected by current anti-virus software. Many free mobile applications include malware that can hide deep within devices. The historic, signature-based approach to anti-virus is not likely to be effective for mobile devices.
**Recommendation:** Organizations should take a multi-tiered approach to securing their mobile devices. Implement a device management solution to manage security policies. Many device management solutions support allowing/blocking specific applications. Some solutions allow organizations to restrict application downloads to a private marketplace that contains only approved, reviewed applications. Use an encrypted email solution to prevent access to corporate email data in the event that a malicious application copies the device contents to a remote location.

10) **Short Message Service (SMS) Attacks:** Short text messages to phones and other mobile devices have increasingly become a vehicle for malware. It is one of the easiest ways to infect a phone. If the user clicks on a specially crafted message, malware can be deployed to the phone providing full remote control of the device.

**Recommendation:** Encrypt the phone’s memory and storage. Use security software that blocks this type of malware or turn off SMS if security is more important than this convenience.

**Conclusion**

While these threats are common, there are others that are cause for concern, such as jailbroken phones, which represent an additional level of risk. Jailbreaking a phone can potentially allow installation of network access applications and other peer-to-peer programs, that attackers can use to introduce threats into the enterprise system. The jailbreak process itself is an exploitation of vulnerability in the device, and there are no guarantees that the groups who craft the jailbreak exploits do not load malicious software as part of the process. Jailbroken phones represent further risk, since applications can be created to report back false results to the device management systems and other security tools in use in a corporate environment.

In the world of higher education, as in many industries, data breaches are common. To stay protected, security strategy must consider the entire institution as well as mobile devices and user behavior. It cannot be limited to single point solutions that are isolated from a holistic strategy that drives security planning and resourcing throughout the organization. Despite the risks and misalignment of security goals that many education institutions face, they can significantly improve their risk posture through a combination of strategic planning for incident response, conducting risk assessments, and implementing controls based on a strong understanding of the institution’s unique infrastructure, network architecture, and mobile device usage patterns.

The bottom line is that while mobile devices introduce a new set of risks to your environment, they can also improve productivity, build morale, and help establish a balance that attracts and retains the talent and student base needed to position your institution as progressive and innovative. The key is an ongoing practice of governance, education and awareness.

For more information about Dell SecureWorks, visit [www.secureworks.com](http://www.secureworks.com)