Small Business, Big Threat

Security Best Practices for Mobile Devices

Background & Introduction

The following document is intended to assist your business in taking the necessary steps needed to utilize the best security practices for you and your employees mobile devices.

This document discusses the most basic security practices that **ALL** businesses should be following as a baseline. If you feel you fall into a more complex category it's highly recommended you contact your IT service provider for further guidance and assistance.

This is not a comprehensive list of all possible security procedures, as many advanced IT security needs depend on the nature of your business and whether or not your business has industry compliance requirements.

Top threats targeting mobile devices

- **Data Loss**
  An employee or hacker accessing sensitive information from a device or network. This can be unintentional or malicious, and is considered the biggest threat to mobile devices.

- **Social Engineering Attacks**
  A cyber criminal attempts to trick users to disclose sensitive information or install malware. Methods include phishing, SMishing and targeted attacks.

- **Malware**
  Malicious software that includes traditional computer viruses, computer worms and Trojan horse programs. Specific examples include the Ikee worm, targeting iOS-based devices; and Pjapps malware that can enroll infected Android devices in a collection of hacker-controlled "zombie" devices known as a "botnet."

- **Data Integrity Threats**
  Attempts to corrupt or modify data in order to disrupt operations of a business for financial gain. These can also occur unintentionally.

- **Resource Abuse**
  Attempts to misuse network, device or identity resources. Examples include sending spam from compromised devices or denial of service attacks using computing resources of compromised devices.

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation.

Small Business, Big Threat

- **Web and Network-based Attacks**
  Launched by malicious websites or compromised legitimate sites, these target a device's browser and attempt to install malware or steal confidential data that flows through it.

When considering the use of mobile devices, the following should be considered:

- How are these mobile devices used, from a business and personal perspective?
- What limitations need to be imposed on the company's mobile device usage through policies and enforcement?
- How can we monitor the network to ensure that these policies are being enforced?
    - Make sure policies are tailored to employees' specific devices, roles and locations.

Best Practices

- **Choose Mobile Devices Carefully**
  Not all devices are created equally when it comes to security. For example, iPods were built for general consumers not concerned about security and were therefore less inherently secure than was a BlackBerry device designed for enterprise users such as law enforcement; Android and Apple smartphones are designed to be fairly secure, though not to the level that Blackberry devices were/are. Tell employees what devices your company will support and allow to have access to company data, and instruct them on the required procedures for getting them set up properly. In most cases it is recommended that you have a mobile device professional do the setup unless you have in-house expertise for this.

- **Update mobile device software and mobile apps**
  Most mobile device apps and operating systems will provide you with a notification when an update is required; additionally most mobile devices will enable you to set up the phone so that updates will automatically be implemented without you having to take any action – this is optimal. This way your operating system and mobile apps will always be updated (including any security updates the developers have made) so that you are as protected as possible.

- **Install Anti-malware software on all mobile devices**
  New malware threats targeting operating systems such as iOS (Apple/iPhone) and Android (Google) are being discovered and exploited every day. Security software must also be updated and maintained just like any other software. Company policies should make this a mandatory requirement for any employee that uses a mobile device for business; whether a personally owned or business-owned device. If it is going to access company data, the installation of **an approved** anti-malware software must be a requirement.

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation.

Small Business, Big Threat

- **All mobile device communication MUST be encrypted.**
  Today's wireless [Wi-Fi] communications are very easily intercepted allowing for data to be stolen or manipulated, therefore it is imperative that employees utilize encryption on all communications of text or any type of data from their mobile devices. Seek a technology professional for guidance on achieving this and providing the necessary training to your staff.

- **Company polices must require strong authentication and passwords**
  Some newer mobile devices include local security options such as built-in biometrics – fingerprint scanners, facial recognition, voice-print recognition and so on; when available, you should insist that these options be utilized. In the absence of these newer options, it is imperative to make sure that strong authentication and passwords are set up to ensure possession of a mobile device does not automatically grant access to important information and systems. Again, be certain to have your employees choose the strongest password that the device will support.

- **Plan for the worst – lost or stolen devices**
  In addition to the best practices stated above, it is recommended that company mobile devices automatically wipe the device of its internal storage information in the event of being lost or stolen. This will aid in preventing data from being accessed in such a situation. There are mobile device management systems available that will provide this capability, most mobile device security software also provides this capability, or as a final resort – in most cases the carriers will implement this for you (but don't expect the process with them to be easy or quick, and likely also costly).

- **Third-party Software [apps]**
  Company policies should limit or block the use of third-party software on company-provided devices. This is the best way to prevent possible compromise and security breaches resulting from intentional or drive-by installation of rogue software, replete with backdoors and "black gateways" to siphon information. Unfortunately, this is not really an option if your employees are using their personal devices for work. In the case of company-provided devices it is suggested that your company provide a list of pre-screened, verified, company-approved mobile apps that may be utilized on company devices to keep risks from 3rd party software (apps) to a minimum. If you need assistance in verifying the safety of apps that you want to approve for staff use on company devices, contact a technology professional for assistance.

- **Create separate, secured mobile gateways**
  Be diligent and thoroughly understand what kinds of uses, systems, and applications your firm's mobile device users will require access to and use. Provide a specific gateway for access that is protected with the most up-to-date anti-malware software and other cyber-security tools. These tools should include data loss prevention applications and protocol and content filtering. Most small businesses won't have the technical knowledge to implement this, but should acquire the services of a well-respected technology professional (not your high-school aged nephew, or your

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation.

brother-in-law who took a programming class who is sure he knows what to do!)

- **Require that all mobile devices be "locked down"**
  Company policy should require that prior to allowing employees use their mobile devices for work, they should be configured to avoid unsecured wireless networks, and Bluetooth should be hidden from discovery. When not in active use for headsets and headphones, Bluetooth should be disabled altogether. Again, in most cases, you should employ the use of a technology professional to set this up on employee's devices; you should also do surprise audits of employee devices periodically using a technology professional to ensure that employees are not changing the settings and again putting company data at risk. Employees should be required to permit these audits in order to be allowed to use their personal phones for company business.

- **Perform regular mobile security audits including penetration testing* [pen-testing]**
  This should be done at least yearly. It is recommended that companies hire a reputable security-testing firm to audit their mobile security devices. These firms should be able to help with remediation and mitigation of any issues discovered.

  ****Penetration testing*** is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities including: operating system (OS), service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are useful in validating the efficacy of defensive mechanisms, as well as end-users' adherence to security policies.

- **Monitor your mobile device battery usage**
  Notice how long your battery lasts. If you notice a significant change in decreased battery life note that malware will often cause this and you should have a professional examine your device as quickly as possible – and refrain from using the device any further until it has been determined to be "clean" in order to minimize the risk that hackers can gain access to company data.

- **Don't Use Public Wi-Fi**
  Public Wi-Fi is easily breached and therefore is often utilized by hackers who may appear to be busily working in the coffee shop next to your employee – and they may be busily working – stealing your company data off your employee's cell-phone or tablet! Instruct employees to avoid using public Wi-Fi in all circumstances.

- **EDUCATE, EDUCATE, EDUCATE**
  Mobile device security should complement and amplify your general IT cyber-security policies. Participation in cyber-security education should be required for all employees. Explain exactly how devices are deployed, and what are the allowed configurations and applications. Tell, show, and put it in writing!!! If you don't feel confident doing this education, utilize the services of a technology professional to do so – and if need be, videotape them to use at the time of future

hires.

- **Upgrades**
  Be certain to wipe any mobile device that will be re-purposed or turned in to a vendor for upgrade. Deleting content from the device is not enough; follow the device instructions to take the device back to original factory status. If you can't find the information; ask your cellphone carrier or hire a professional to do it for you, otherwise data may remain that you may not be aware of. That data may compromise your firm and/or the person who previously utilized the phone. **NOTE:** Jailbroken, rooted, non-manufacturer ROM-based devices may not respond to the wipe command.

- **Avoid opening unexpected text messages from unknown senders**
  One of the newest ways of compromising mobile devices is SMSishing (or SMS phishing – see definition on Q&A doc). This form of attack is when a potential identity thief sends a text message asking for personal or account information. This information can then be used to log into corporate systems, banking or financial accounts as well as send malware. Sometimes, the device is compromised and the owner becomes a victim of "ransomware". Like the term suggests, the device is locked and the owner must "pay a ransom" to regain access.

- **Don't open suspicious emails**
  Don't open an email if anything about it seems suspicious – even if it appears to come from an email or contact that is familiar to you. That person's contacts may have been hacked and they are utilizing their email address to send you and all that person's contacts a virus. Be on the lookout for misspellings in the subject line, odd grammar, all caps in the name or subject line, or anything else that looks unusual. NEVER click on a link unless you are completely confident it is from a trusted source.

- **Ownership is the question**
  Will employees be allowed to use personal mobile devices for company business or will your company provide them with devices to use only for company business? Businesses that provide mobile devices to employees have a greater chance of keeping data safe.

- **Social Media use requires caution**
  Be cautious about accessing links, videos, photos, QR codes, etc. from social media; it's not difficult for hackers to embed viruses or malware in any of these typical social media content items where they can be assured if it is buried in something related to a currently popular topic that it will be opened and shared hundreds if not thousands of times. Since a majority of social media users access their accounts via mobile, this provides them easy, and fairly quick, access to hundreds if not thousands of mobile devices.

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation.

Small Business, Big Threat

Mobile Security - A State of Mind

Mobile device security is only a portion of the security infrastructure a business owner must put into place to protect employees, assets, reputation, and business mission. Taking the appropriate steps to mitigate [reduce] risks and prevent losses will allow vendors, contractors, and employees to take advantage of mobile devices in the workplace. Remember, failure may lead to legal liabilities, penalties, and/or the loss of your business.

"Bring Your Own Device" [BYOD] management (meaning employees use their own devices for work) for a company requires learning about virtual work environments such as "VPNs" or Virtual Private Networks. These stand-alone systems allow employees to work remotely while accessing limited systems, applications, or data. For more detailed information on VPNs, contact a trusted cyber-security professional.

A reliable resource to create a Mobile Device Policy for your company may be found at – http://www.sans.org/reading-room/whitepapers/pda/security-policy-handheld-devices-corporate-environments-32823

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation.