8 Critical Security Measures Every Business Must Put In Place NOW With Mobile Computing

If You Have Given Or Plan To Give Your Employees The Ability To Access Company Data And Systems With Mobile Devices – DON'T...Until You've Read This

James Moore
Technology Solutions Consultants

Technology Solutions That Offer Business Owners Less Worry & MOORE Time to Focus on Running the Business.

Mobile And Cloud Computing: Benefit Or Threat?

There's no doubt about it – the Internet and mobile computing have made our lives easier and our businesses more productive, cost-effective and competitive. But make no mistake about it; the Internet is also a breeding ground for thieves and predators, not to mention an enormous distraction and liability if not used properly. It is causing people to be casual, careless and flat-out stupid about their privacy in an increasingly litigious society where heavy fines and severe reputational damage can occur with one slip up – which is why you cannot be casual or careless about introducing it to your organization. You can't turn on the TV or read a newspaper without learning about the latest online data breach. And mobile devices are easily misplaced and stolen.

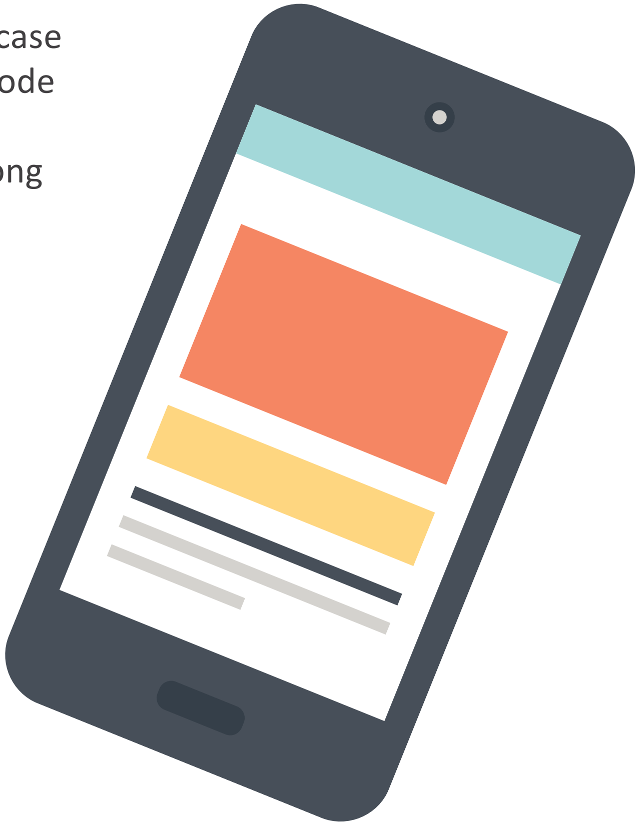
Because of all of this, if you are going to allow employees to use mobile devices – *particularly personal mobile devices* – to access, store and use company data, then it's **critical that you have these 8 security measures in place.**

1. Implement a mobile device policy.

This is particularly important if your employees are using their own personal devices to access company e-mail and data. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR information, or your clients' information, isn't compromised? Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can and cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place. Can the employee use the camera or bluetooth capabilities of the device? Can they save files to a smart card they added? These questions must be addressed in your mobile device policy.

2. Require STRONG passwords and passcodes to lock mobile devices.

Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode be entered will go a long way in preventing a stolen device from being compromised. Also, setting the device to automatically wipe itself if the wrong passcode is entered too many times can help prevent data theft.



3. Require all mobile devices be encrypted.

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that unlocks (decrypts) the data. Sometimes the information on a mobile device can be accessed using special 'diagnostic' tools even if the device cannot be logged into with the passcode. Ensuring the device and smart card are encrypted helps prevent your business information from being taken off the device even with those tools.

4. Install locating software.

If a device is lost or misplaced, being able to trigger the the device to report its location so it can be quickly located could prevent a more severe compromise and all the actions which come with such a device loss.

5. Implement remote wipe software for lost or stolen devices.

If you find a laptop was taken or a cell phone lost, “kill” or wipe software will allow you to disable the device and erase any and all sensitive data remotely.

6. Back up remote devices.

If you implement Step 4, you’ll need to have a backup of everything you’re erasing. To that end, make sure you are backing up all MOBILE devices, including laptops, so you can quickly restore the data.

7. Don’t allow employees to download unauthorized software or files.

One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other “innocent”-looking apps. Preventing the installation of additional software on mobile device may cause the end users some frustration, but it can go a long way toward protecting your business information.

8. Keep your security software up-to-date.

Thousands of new threats are created daily, so it’s critical that you’re updating your mobile device’s security settings frequently. As an employer, it’s best to remotely monitor and manage your employees’ devices to ensure they are being updated, backed up and secured.

The way technology is moving forward today, mobile devices make communicating and working on the move much easier. Like many things in business, you have to weigh the increased productivity with the increased risk of data loss, and you have to take appropriate steps to reduce that risk. At James Moore, we understand and are here to help! As your trusted business advisor, we can help with all of your technology needs, including managing your mobile device security concerns. Please contact us, and find out how our technical staff can help you, 800-455-5676.