BIZCOMMUNITY

Five ways to keep your mobile devices secure

By Aaron Thornton

14 Apr 2015

It seems like every time you turn on the news lately, there are more stories of companies having their data stolen or corporate networks being hacked into.

Image: www.freedigitalphotos.net

In fact, data theft and the hacking of business networks is actually on the rise. More and more of these attacks are originating with lost, stolen, or hacked mobile devices. This is compounded because many business IT departments still aren't sure of how to properly secure phones and tablets, or don't place a high priority on locking down these devices. How can you keep your employees' mobile devices safe?

Here are five ways to keep your mobile devices secure:

1. **A good backup solution**: Before even considering the risk of data theft or other malicious actions, you need to secure your mobile devices against common loss or breakage. A core component of this is a good back-up solution. The ideal solution will be automatic, freeing your employees from having to worry about running a regular backup, and would back things up to a remote cloud server for safe storage. That way if a member of your sales team drops his phone and it shatters, or forgets a tablet at a conference, you don't lose any of the data on that device;

2. **Data encryption**: If you or your employees' device is lost or stolen, the last thing you want to worry about is someone getting hold of your confidential business information. Prevent that from happening with strong data encryption software for all your mobile devices. While most people are okay with using either a short PIN or a pattern key to unlock their phones, such measures simply aren't secure enough for business equipment. Fortunately, many great encryption solutions are available for all makes and models of phones;

3. **Remote wiping**: Even better than data encryption is the ability to simply erase all data on a phone as soon as it's

discovered to be lost or stolen. If you are using a good back-up solution, this shouldn't result in any lost data or productivity. Many software solutions exist for executing a remote wipe, and you should speak with your IT team to find one that best fits your company's needs. Keep in mind, however, that a remote wipe app doesn't preclude the need for good encryption. Remote wipes only work if the phone is turned on and getting a signal. If the phone is out of power, turned off, or out of cell range, it won't be wiped;

4. **GPS tracking**: "Find my phone" apps are now available for every major phone OS, with multiple options to choose from on each app store. These apps utilise the GPS antennas in your device to pinpoint its location accurately if the phone or tablet has been lost or stolen. These can be invaluable for locating and recovering lost devices, and can make it much less likely that a stolen phone makes it very far. Unfortunately, the phone needs to be powered on and have an open view of the sky (as well as a network connection) for these tracking apps to work. Still, the odds of recovery are much higher with a phone finder app than without one; and

5. **Lock screen contact info**: If your lost phone is found by someone, you want them to be able to get in touch with you without having the ability to root through your device and figure out who you are. This is where 'lock screen contact information' comes in. If you don't have some sort of label with contact info on your phone, you should at the very least provide an easy way for people who find your device to contact you and return the mobile device back to you.

ABOUT AARON THORNTON

Managing Director at Dial a Nerd

- #BizTrends2020: SME technology in 2020 - a path to efficiency - 6 Jan 2020
- Are you leaving the front door open for cyber criminals? - 16 Oct 2019
- Why tough times call for technology-led innovation - 10 Sep 2019
- What every business owner should know about migrating to the cloud - 3 Aug 2018
- Three security issues to consider when using public Wi-Fi - 20 Apr 2015

View my profile and articles...