Your Biggest Security Risk is Close at Hand

By Arley Turner

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity

According to an article titled "Planet of the Phones" featured in the 2/25/15 edition of The Economist, by 2020 over 80% of adults will have a smartphone, and 80% of current smartphone users reach for their phones within 15 minutes after waking up. I am one of them. After waking up I immediately reach for my phone. I glance at the weather forecast, peruse the headlines, and check my favorite social media sites. I even check my work email, all before I get out of the bed.

While checking work email from my personal device is super-convenient for me, are there security risks for my employer? Introduced in 2007, the iPhone has become the most used electronic device in the workplace. And while at first it was hard for criminals to hack into smartphones to steal valuable data assets, this is no longer the case. New smartphone malware is created every day, and the theft of data from your smartphone is a very real risk. The biggest problem is that the average user isn't very concerned about the security risks associated with their handheld connection to the world. According to the article, "The Spy in Your Pocket," featured in the same 2/25 edition of The Economist, "Consumers have learned the hard way that personal computers are vulnerable, but that realization has not yet sunk in for their phones. Smartphones use a single cable to charge their batteries and to transfer data. That means that plugging in to unfamiliar charging points can be a security risk."

With too little concern about these security risks, employees at small and large organizations alike are often unsupervised in their use of personal devices for important nonprofit business. And if your organization permits the use of personal devices for organization business, your critical and confidential data may be carried on and wiped off these devices. This leaves it up to organizations to enact policies to help protect their data. These policies, commonly referred to as BYOD (Bring Your Own Device) Policies, are the best way for an organization to limit access to privileged information and applications. Here are a few tips on implementing a strong BYOD policy at your organization:

Smartphone Safety Risk Tips

Don't be Naïve – The first step is to stop naively believing that use of personal devices for work purposes is akin to a "free lunch." Or remind yourself that there is no such thing as a free lunch! While you've avoided the cost of purchasing smartphones for your staff, the cost-savings may have a surprising, hefty price tag in the form of exposure to data loss.

Set Clear Expectations – Many staff simply don't realize the security risks associated with smartphones. By raising awareness about this issue as you develop and roll out a new BYOD policy, you'll increase the likelihood of buy-in. As you develop your policy, be explicit about what organization information may and must never be accessed on personal devices. For instance, you may allow employees to retrieve and send email messages from their phones, but strictly prohibit signing on to the human resources or donor databases, both of which may contain personally identifiable information (PII).

Enhance Security – Does your entity regularly encrypt data prior to sending it via mobile devices? Do you require employees to download additional anti-malware software to their personal devices? These are extra security steps you can take to help protect the confidential and PII information in your nonprofit's possession. Also, consider whether it makes sense to install remote-wipe and GPS location finders onto employee-owned mobile devices. That way if the device is stolen or lost you can help find it and remove any data that could expose your entity to legal claims, or worse. Keep in mind that before taking these steps you should obtain written consent from the owner of the device.

The most important thing to remember with any BYOD Policy is that technology isn't static: the technology landscape is always changing. Risks associated with smartphones today may be amplified when wearable technology becomes the norm. Remember that flexibility is an essential component of your BYOD policy. To minimize the risk of your policy quickly becoming dated, focus on security concepts, rather than naming specific devices in your policies.

For information about the Nonprofit Risk Management Center, visit www.https://nonprofitrisk.org/ or call 703.777.3504.