Why We’re Cautiously Optimistic about Using Mobile Devices at Work

Posted on Aug 14, Posted by Ira Greene Category Technology

As expected, mobile technology is a consistent part of daily business operations for many companies around the world. Employees love taking advantage of the mobility these devices offer, making their home office just as useful as their in-house workstation. However, a mobile device management solution needs to be strictly adhered to in order to optimize security and guarantee that a stray smartphone doesn’t expose your data to unexpected eyes.

One of the best ways your business can approach mobile devices is by consulting Lighthouse Technology Solutions’s technology experts. We can work with you to build the ideal Bring Your Own Device (BYOD) solution, designed to protect your business and approach mobile devices in an organized, secure way. In fact, with the cloud increasing access to data and mission-critical applications, it’s no wonder that businesses are skeptical of this yet-emerging technology, despite the incredible advantages it brings to the table.

The largest reason that businesses invest in a cloud IT solution is to make their company’s resources more accessible for their entire organization, from approved devices that adhere to a BYOD policy. This means that your end-users can access documents and files from any of their mobile devices, including laptops, smartphones, tablets, and more. With all of these devices capable of accessing information both in and out of the workplace, it’s reasonable to treat the BYOD trend with a level of skepticism.

Take, for example, the average virus infection. An employee visits a site on their smartphone,

which infects their device with a virus or some sort of spyware. If this device connects to your network, this infection can become much more widespread. This kind of risk to your network’s integrity is a worst-case scenario, but is completely avoidable under the right circumstances.

The best way to protect your network and its cloud infrastructure is to make security a priority for your BYOD policy. A good mobile device management solution should be capable of limiting certain applications’ access to confidential information. It helps if you’re able to blacklist certain apps from accessing your data, and whitelist approved apps that can do so without risking the integrity of your network. This should be done, especially if you’re the one providing your team with mobile devices.

The basics will be better than nothing, but to truly optimize your network’s security from the BYOD menace, you need to integrate a much more comprehensive security solution. By limiting access to data based on user permissions, you’ll be more likely to minimize data leakage and keep your network relatively free of potential threats. Give Lighthouse Technology Solutions a call at 703-533-LTSI (5874) to learn more about how you can protect your network.

Tags: Tagged in: Mobile Device Management Mobile Office Small Business