Cybersecurity In A Mobile World

By Danny Pehar

In the 1990s, if someone told you they wanted to talk to you about corporate security, you most likely thought they were going to talk to you about video cameras and security guards. However, as we've changed the way we conduct business, we've also changed the definition of corporate security.

As we started storing and accessing our corporate data online, the definition of corporate security needed to include considerations for cybersecurity. As we started making that information extremely mobile, we needed to add to the definition of corporate security again to include mobile security.

Information is now more mobile than ever. This mobility brings us so many opportunities. As is often the case with opportunity, however, mobility also brings with it an increase in risk. The more places we store our data, the more we increase points of vulnerability for cybercriminals to capitalize on.

The hardest part about securing mobile data is that it represents two main points of vulnerability — the first being the device itself. Mobile devices are light and easy to hide, carry, steal and resell, making them very tempting for thieves. The second point of vulnerability is the actual sensitive data that may be stored on the device itself. Losing a mobile device to a criminal means that not only did you lose an expensive piece of equipment, but you may have also allowed a criminal to gain access to your sensitive data, which could lead to far worse problems than the theft of the actual device.

With that being said, here are some great tips for mobile security to help keep you, your colleagues and your loved ones safe:

• Review your company's security policy to know which devices you are allowed to use at work.

• Always encrypt sensitive information if it is put on any storage media.

• Immediately remove sensitive information as soon as it is no longer needed.

• Keep storage media in locked drawers when not in use.

• Don't insert unknown mobile media, such as a USB key, into your computer.

• Devices bought at stores can come with malware on them. Always run anti-malware software and a firewall on your computer.

• Configure mobile and IoT devices for security before using them.

• When in public, use a wall adapter instead of a USB charger to charge USB devices because this will eliminate the chance for a transfer of malware.

• Avoid file-sharing sites, which often have malicious files and illegal content. Instead, get content from trusted vendors.

• Only connect personal devices to your corporate network when it's allowed by company policy.

• We can't prevent all theft in our lives, but that doesn't mean we have to make it easy on the criminals by leaving mobile devices in plain sight in vehicles. If possible, mobile devices should be left locked in your workspace unless you carry them with you. If you must leave a device in your vehicle, store it in the trunk before you arrive at your destination.

• Remember, someone does not need to steal your sensitive data for you to be compromised; they just need to be aware of it. With that in mind, use a privacy screen protector, or position yourself away from others to keep others from viewing sensitive work.

It's important to remember that we carry entire computers with us in the palms of our hands, and those computers are loaded with sensitive information, making them very tempting for criminals to steal.

In the best interest of yourself and your loved ones, when it comes to mobile data, proceed with caution.