Cybersecurity And Your Workspace

In previous articles, I have discussed how cybercriminals love to get their hands on our sensitive data because it's the newest form of currency and is worth good money to bad people. When a cybercriminal gets their hands on our sensitive data, it represents a great payday for them and creates a nightmare for us.

There are a few places of vulnerability where a cybercriminal can easily get their hands on this data, and one such cybercriminal paradise is your workspace, which is a hotbed of sensitive information.

And yes, this article is a bit different than usual cyber hygiene-focused strategies because I am not referring to a digital pathway from the criminal to our data, but rather a physical one and its effects on our digital lives. But make no mistake — the vulnerability is real.

The truth is, cybercriminals do not limit their actions to digital ones. Many times they incorporate a physical element to their scams that could include making a fake phone call to trick someone into giving out too much information or physically walking into an office location to steal very expensive and easy-to-carry mobile devices or to spot and steal sensitive corporate information.

When your wallet goes missing, it’s very easy to know that something valuable to you has been compromised, allowing you to immediately do something about it. However, the tricky part is that when it comes to our data, a criminal doesn’t need to actually take it away in order for them to do nefarious things with it; they simply have to know it. And with everyone walking around with cameras on their phones, it has never been easier for cybercriminals to take a picture of sensitive information left on a whiteboard or calendar or even notes on someone’s desk — not to mention all the overlooked but often incredibly sensitive information left on copier trays, fax machines and printers.

The workspace is a gold mine to a criminal, containing not only expensive merchandise, but unguarded sensitive information left on whiteboards, calendars and papers.

It is incredibly easy for strangers to simply walk into workspace environments, dressed very professionally, and not look suspicious at all. They can simply walk in wearing a suit and holding a briefcase and walk out with stolen merchandise or having copied sensitive information.

Keeping that in mind, here are a few ways to help make things a little harder on the next cybercriminal who attempts to score an easy win with your sensitive information.

Remember to ask yourself these three questions when you leave your office:

1. Do I have my mobile device?

2. Is my computer/laptop either physically locked or with me?

3. Do I have my keys and/or access card with me?

It is difficult to stop a determined criminal, but remembering to ask yourself these questions will at least not make it easy on them.

Never do the following:

• Never leave sensitive information exposed on a whiteboard, calendar, copier, fax or printer tray.

• Never use a newly found USB key. No matter how tempting it may be to attach a newly found USB key to your computer, it could be loaded with malware and incredibly dangerous.

• Never write down your password.

• Never put unencrypted, sensitive data on something like a USB key.

• Never discard sensitive information in the trash without properly destroying it.

Remember that although we all love a comfortable workspace, when it comes to the safety of ourselves, our families and our loved ones, it’s best to not be so comfortable that we drop our guard with our sensitive information.