Cybersecurity: Easy steps to protect you, your workplace, and your home

Author : Cat

Date : October 17, 2017

When I started my career as a software developer, the word *cybersecurity* was thrown around as technical term describing how computer data was encrypted and protected within an electrical system. Fast forward a few decades and now *cybersecurity* affects everyone who touches a digital device. The problem is many people still feel like it's technical issue that they don't need to worry about, but that's not true.

Cybersecurity is everyone's issue because the biggest hole in your safety, the safety in your home, and at your place is of work, is YOU, the person using it. October was designated Cyber Security Awareness Month to help bring attention to these issues but they are certainly relevant all year.

Personal Cybersecurity

Whether you carry a phone, a tablet, a laptop, or a combination of devices, our lives have become tightly intertwined with our devices. In many cases, your device is an extension of you, holding our appointments, health data, maps of places we've have been. It is critical that you keep the data, and access it to it, safe from prying eyes.

Top Safety Tips:

- Passwords can be guessed or broken, but by using Multifactor authentication, criminals cannot get in your account with a password alone. Learn more about what it is and how to set it up.
- Public WiFi can be easily intercepted by prying eyes. If you are using **public WiFi, do not enter your passwords or credit card numbers**.
- Hackers love to get to your data through programs they put your on device. Many of these come from downloads, including apps and games. **Only download from reliable sources and websites.**

You should know:

When you cross a border with a cell phone, the border guard has the right to ask you to unlock your phone and show them your data, including social media accounts. Keep this in mind when you travel.

Cybersecurity at the Workplace

Your company could, and should, have software security in place to protect against data breaches. But, the biggest risk in company security is spearphishing through social engineering. The means that criminals are using personal data to target specific people (spear phishing) and then using that data to convince other people to hand over information. This can be done through fake sign-on pages sent through email or via phone calls to coworkers. All with enough background data to be convincing.

Top Safety Tips:

- You should be aware of the major scams and ways that hackers access your data. Be sure to **read our** glossary of scams at least once.
- Educate staff about cybersecurity with workshops and/or seminars.
- Separate personal from professional. **Do not make personal social posts with pictures from within your office** that can be tagged or be giving away internal information in the background.

You Should Know:

If you are working a device provided by your company, such as a laptop or phone, your company owns the device and thus the data. They have rights, and usually the ability, to access that data

whenever they want to. Be wary of that before using it for personal pictures, searches, or apps.

Cybersecurity at Home

The Internet of Things, or IoT, is a collection of all things that are connected. Not just the internet and phones, but FitBits, Nest thermostats, and most new model cars. Having all this connectivity has provided amazing things but also puts other pieces of the network at risk. Each IoT device has access to the network you've put it on and/or your personal data. It is important to know how to protect the data the devices hold as well as protect them from each other.

Top Safety Tips:

- **Learn and understand about the** Internet of Things so you have a better idea of what is connected and how much data you are going away.
- **Change the default password on all IoT devices** that you have connected to your home network.
- **Protect your WiFi Access with a password**. An open WiFi router will allow anyone access to any device on your system.

You Should Know:

Personal digital assistants like Siri and Alexa are available to answer questions on voice command. That also means they have to be listening at all times to be ready for their command word. As such, the data they store could be requested by law enforcement if ever a crime were to be committed in your home.

Technology is intended to assist us with our daily lives but, just like a car, we need to know how to use it safely to make sure it is more helpful than it is harmful. Take time to protect yourself, your business, and your home. Stay Cyber Aware.