Cybersecurity Defense Begins With Awareness

I've been in the cybersecurity industry for most of my adult life, and throughout that time, I've had the pleasure of working with some of the best digital forensics experts in the world. Digital forensics experts are the people who get called in after a cyber breach to figure out what happened, among many other things.

For about 20 years now, every time I've had the pleasure to sit down with one of these professionals, I pick their brain about what they see as the most common thing that allows cyber breaches to keep happening. Over and over again, they tell me that hackers are tricking people into doing things they shouldn't be doing, whether it's clicking on a corrupt link, downloading a corrupt file or willfully giving sensitive information away to the wrong person.

Hackers are hacking people, and it seems to be working well.

It is this knowledge that has consistently led me to preach about cybersecurity awareness. Throughout my journey of spreading this awareness, I am often met with people who are convinced that they don't need to be aware of the dangers and threats brought on by the digital age. Among the various objections to cybersecurity awareness, I find that a common misunderstanding is that having a Mac or an iPhone means you're protected from threats.

If you ask any cybersecurity expert out there, one of the biggest fallacies with regards to cybersecurity and Apple products is that a Mac can't get a virus. They certainly can. Apple products can get viruses and malware just like any other technology. Not too long ago, there was a line of text that could brick your iPhone, and in another case, malicious apps were found in the Apple App store.

But even if Apple products weren't vulnerable to viruses like the rest of connected devices, would you be cyber safe if you had one? Absolutely not.

Imagine if you lived in the most secure house in the world, with an impenetrable door and an impenetrable lock on that door. Your incredibly impenetrable house will do you little good if the criminal on the other end of that door tricks you into willfully opening the door every time they are there to rob you. And that is exactly what's happening with the threats brought on by the digital age

— meaning that it doesn't matter if the technology you have is impenetrable to a hacker (which it's not) because hackers are not hacking tech anymore. They are hacking people.

We cannot rely solely on technology to protect us.

If a hacker reaches out to us pretending to be someone we know or disguises a fake website to look like a legitimate one, and we willfully give them our information, passwords, gift cards, money and so on, our technology will have a hard time protecting us. Regardless of the technology you have, the only true defense for these threats, and the absolute best protection out there, is good cybersecurity awareness.

The best way to develop cybersecurity awareness habits is to first understand that you are, in fact, a target for cybercriminals. For the most part, as a society, we seem to understand that the impacts associated with a cyber breach are pretty bad. I find that we just don't seem to believe the probability. No one seems to think it will happen to them.

Understand that, if you have data, then you do have cyber risk. If you truly believe and understand you and your data are at risk, then you are already well on your way to becoming cybersecurity aware.

We must take a proactive approach.

All cybercrime begins and ends with what the cybercriminal is targeting: your sensitive information. One of the best tips for cybersecurity awareness is to make sure you are aware of what information of yours is sensitive and remain especially careful with where you put it and who you allow to access it.

I find that hackers love to play on our emotions, in particular. They love to get us really scared, happy, sad or angry so that we are not thinking straight. If you come across someone asking you for your sensitive information, and they invoke a strong emotion out of you, stop for a second, take a breath and ask yourself, "Was I expecting this? Does this make any sense at all?" If it doesn't make sense, do not give away your sensitive information, even if it seems like you know the person asking for it.

Leaders within organizations need to help their employees understand why being aware is so important. And the best way to do this is by making your message specific to your audience. When encouraging employees to follow best cybersecurity practices, don't tell them it will help keep the company secure; rather, tell them how good cybersecurity hygiene will help protect them and their families. I find that a person's willingness to learn about any topic will greatly increase if they understand how the lesson will benefit them personally.

The fact of the matter is that, in a digital world, our data is everything, and it is incredibly exposed. We cannot afford to be so naive to think our technology alone will protect us. Let's take the safety of

our data to the next level and put the power of protection back in our own hands by spending the brief time required to be more cybersecurity aware.

By Danny Pehar