



### DON'T GIVE A GIFT TO CYBER CRIMINALS

Cyber criminals spend their time looking for ways to steal private information and money. And unfortunately, they are rather good at it.

That means we have to be extra vigilant and do our best to remain safe.

Most firms have a cyber security team that works hard to keep things secure. But as long as we think they are solely responsible for maintaining a safe environment we are giving a gift to the cyber criminals. Cyber security is everyone's job. Yes, yes, I know, you aren't trained in cybersecurity. And the cyber security team isn't helping you do your job so why should you help them do theirs?

The answer is because you do have a responsibility to keep company and customer data and information safe. Think of the cyber security team as making sure the windows and doors of the building are strong and secure. But if someone leaves the door or a window unlocked, or even wide open, then all the locks don't mean a thing.

Everyone needs to understand phishing, vishing, and the other social engineering techniques used to get past the defenses. Because if you fall for these, it is leaving the door open. The criminals don't have to break in, they have been invited in by you providing your login credentials. Or by allowing the download of malware onto your computer which will spread and cause damage. It may even be ransomware which can bring your company to a halt.

We all use the common applications provided by the company or chosen by us for personal use. For instance, Microsoft Office 365, Virtual Private Networks, VPN, and so many other packages.

But how well do we know them? The bad guys spend their time delving into them looking for weaknesses or other ways to get in. While we are not expected to be experts in these packages, after all we only use them to do our jobs. But we do need to understand the steps that users are required to take to keep things safe.

No, they are not an imposition on our time or an interference in getting our jobs done. They are part of our jobs in protecting company and customer information.

Virtual Private Networks, VPN, are used to provide a secure network connection when out of the office. With the rapid shift to working from home due to the pandemic, VPNs were stretched to their limits. The result is no capacity, delays, and slow response times. I'm sure the IT and cyber security teams are well aware of the challenges. But do not circumvent the VPNs or any other precautions. You will not like the results if you are the one leaving the door open.

The holidays are when we are extra busy and looking for that last gift or bargain. Or an update on pandemic news. Cyber criminals know that in the rush we often let our guard down. Don't give them that gift.

We have only scratched the surface of cyber security risks. Speak to your IT or cyber security teams about what they recommend and ask for training. They will appreciate it. And having them as friends is a good thing.

We at AIM Cyber wish you happy and safe holidays.

To learn more about cyber protection and education contact AIM Cyber at [info@AIMglb.com](mailto:info@AIMglb.com) or call (888) 773-1920.