Cybersecurity And Sensitive Information

In previous articles, I've talked about how everyone is a target for cybercriminals. I've talked about how hackers don't care who you are, how young or old you are, or even how much money you have or don't have. To a cybercriminal, you and your loved ones are the perfect targets.

But what specifically are they targeting us for? The answer is simple: Cybercriminals are targeting us for our data, but more specifically our sensitive information.

The best way to protect ourselves is to understand exactly what the bad guys want. For most average citizens our sensitive information fits into three main categories.

Category No. 1: Sensitive Personally Identifiable Information (PII)

PII is considered sensitive when it can uniquely identify an individual. Things like your Social Security number, driver's license number, passport number, full credit card number, financial account numbers, birthdate and birthplace, and citizen or immigration status are considered PII.

Category No. 2: Protected Health Information (PHI)

PHI includes, but is not limited to, any past, present or future information about a person's health status, medical diagnoses, health care provided and payment for medical services.

Cybercriminals love selling health information on the dark web. If your credit card gets compromised, all it takes is one phone call to your credit card company to cancel your card and get a new one. Not so easy to do with your health information, and hackers know this.

Category No. 3: Confidential Information

Confidential information is sensitive corporate information that, if exposed, can damage a company, either directly or indirectly. Think about KFC's secret

formula. If it was publicly exposed, it could be very advantageous to competitors.

Information that is often considered confidential might consist of trade secrets, financial records, contracts and credit cards, strategies, customer lists, plans and pricing, salaries and employment records, physical plant details, designs and prototypes and merger or acquisition plans.

How To Treat Your Data

Now that you know what sensitive information is most valuable to a criminal, it's very important for you to understand that you must treat this very sensitive information the same way you would treat cash, meaning, if you were at Starbucks and you had a big bag of money sitting on the table, you probably wouldn't leave the bag of money unguarded while going to get a refill on your coffee.

Keep that same way of thinking when it comes to sensitive information. Using the Starbucks example, if you are filling out some sort of form and it contained all kinds of sensitive information, don't just leave that data unguarded as you go get that refill. Sensitive information is just as valuable as cash, except it's more vulnerable.

Still using the Starbucks example: If a criminal wanted to steal your bag of money, they would have to make an obvious attempt to take it. You would know fairly quickly that you are being compromised, and you can either shout for the police, shout at the criminal or call for help. Whereas with data, someone does not need to physically take it from you — they just need to copy, record it, overhear it, see it and know it. And just like that, the wrong person has something of yours that's worth a lot of money, that can cause you a lot of trouble in the wrong hands.

When it comes to sensitive information, it's important to:

• **Understand it.** Know where your sensitive information is and more importantly who has access to it.

• **Lock it.** If there is sensitive information inside and you're not present, it needs to be physically and/or password locked.

• **Properly destroy your data.** When getting rid of something that contains your sensitive information, whether it be in electronic form or just on paper,

make sure you have taken the necessary steps to ensure that the data has been properly destroyed.

• **Remove it when it's no longer needed.** If you don't have it, it can't be stolen from you.

• **Watch what you say.** When dealing with sensitive information, remember, it doesn't need to be physically taken from you. It just needs to be known by the wrong person.

• **Be careful with what you post online.** Way too many people put way too much of their sensitive information on their social media accounts, making it very easy for a cybercriminal to get their hands on it.

• **Be mindful of third-party apps.** When we click accept to terms and conditions of online free apps, we give permission to third-party organizations to gain access to our sensitive information.

Bottom Line

Remind yourself that sensitive information is the new gold to cybercriminals, and it needs to be treated as such. Use the tips in this article to protect you, your colleagues and your loved ones.