A New Opportunity For Cyberscams

There's a cybersecurity threat so troublesome that not even some of the best cybersecurity technology can stop it. It's called psychology, and it's used in any number of cybercrime attacks.

Cybercriminals and scammers use psychological games to trick potential victims into becoming actual victims. In many cases, hackers leverage newsworthy crises in their scams, and I predict the coronavirus outbreak is no different.

As the coronavirus death toll rises, I believe we can expect to see scams from fraudsters using the coronavirus outbreak to play with our emotions.

There is a lot of talk about malware, ransomware, spyware and any other type of evil ware in the media, but it's important to remember that one of the best weapons a cybercriminal can use is psychology. Understanding how they use these tactics against us and how to respond is a must.

What will these scams look like?

In my experience, I've seen firsthand how common it is for cybercriminals to play with our four main emotions (i.e., fear, sadness, anger and happiness). They trick us by sending false information that is designed to look real. In the context of the current coronavirus outbreak, here some examples of what I expect these scams could look like:

• **When cybercriminals use fear**, the messages may look like something like this: "Don't get sick! Click on the following link for safety measures on how to avoid the coronavirus."

• **When they use sadness and anger** they are trying to take advantage of our good nature by sending us a message that looks something like this: "Please help others! Donate so we can find a cure for the coronavirus outbreak by clicking here."

• **When they use happiness,** the message may look something like this: "Get rich quick! Buy stock in this company that just created the coronavirus cure."

How can we leverage logic?

As Spock from *Star Trek* often eludes to, our emotions can be the enemy of logic. In many cases, the difference between being scammed and not being scammed is the 10 seconds it takes to pause, take a deep breath and ask yourself whether this makes any sense at all.

Sometimes simply by taking a deep breath before we react, we can more easily spot the scam being presented to us.

It's important to understand that cybercriminals will use multiple forms of contact to reach out to us, such as text, email, phone and even office walk-ins.

Ask yourself these questions.

Keeping that in mind, when someone reaches out to you asking for sensitive information, to click on a link or download an attachment, especially if it relates to the coronavirus or whatever the latest newsworthy crisis is, ask yourself these questions when you examine the message:

• Did you expect the email, text or phone call?

• Did you expect an attachment or link?

• When you hover over the "from" address, is it different than what it claims to be?

• What's the sender's address?

• Does the sender's address make sense for the message being sent to you?

• Are there strange typos or any wording that doesn't make sense?

• Does the email play with your emotions?

• If it's from a friend, is it from their usual address? Are they asking for something strange?

• Does the message make any sense at all?

If you have any doubts, just delete it.

Always remember, never click on a link directly in an email or text sent to you. Always open a separate search window and research the site directly.

If someone is using a URL shortening service like TinyURL and wants you to click on their link, make sure you use a URL lengthening service so you know the link address before you click on it.

Never call a phone number directly within an email or text sent to you, even if it's seemingly from a friend. Instead, research the number yourself.

Cybercriminals will use all sorts of tricks to fool us, but with caution, patience and the tips learned from this article, you can help protect yourself, your colleagues and your loved ones.

By Danny Pehar