How To Keep Cybersecurity Awareness Real In A World Of Fake News

As a cybersecurity professional, I often preach to people about how the best way to prepare yourself to prevent, detect, and respond to cybercrime is to stay aware of cybersecurity best practices and to keep your eyes open for cyber scammers and deception.

That being said, how do you avoid being deceived by cyber scammers and fake newsmakers when the very goal of the deceiver is to make sure their deception goes unnoticed?

The concept of deceiving people with cons, scams, crimes, gossip or fake news has been around for a long time. What makes it more destructive now is that not unlike most of the world itself, it's powered by digitally connected technology, allowing culprits to reach audiences on a worldwide level.

So to help keep you aware, informed and secure, here are four ways to stay ahead of what is real and what is fake.

1. Always make sure to check your source

If you come across something online that you either strongly agree or disagree with but you've never heard of the source, before you share the information with your network, click on a dubious link, or give the would-be scammer your personal information, do yourself a favor and find out whether the source is legit.

If you get an email provoking a particular emotion from you, like your boss asking you to spend corporate dollars on a gift card, reach out to the person in question and ask, "Hey, are you sure you want me to do this?"

If it's an article, do some research on who the author, creator or publisher of the content is. What else have they done? What are their credentials? Are they a professional in their field? Are they someone who has truly researched the

topic in question or just a person with a blog and some time to spare? Remember, it's not just about what is being said, but who is saying it.

Just like fake newsmakers, cyber scammers rely on us not checking our sources.

2. Pay attention to quality

Whether you get a text or email asking you for sensitive information from a would-be scammer or are reading an article that is provoking an emotion from you, see if you can spot numerous spelling errors, lots of caps or other amateur writing techniques like overdramatized punctuation. Poor quality in writing is a sure sign of cybercriminals and fake news.

3. Do your own research

If you receive a message telling you that your bank account has been compromised, open up a separate search window and do some research on whether you can find information about your bank being compromised anywhere else. A story like this would be posted elsewhere. Alternatively, you can phone the bank in question — not from the number listed in the message sent to you but by calling a number you've looked up yourself.

It's a similar tactic with regards to a story you come across online. What facts is the story referencing? Can you find those same facts through your own research? Who else is reporting this story and these same facts? What experts are being quoted in the story, and what are their credentials? If you are reading a fact that doesn't exist anywhere else and can't be corroborated by a credible source through your own research, chances are it's fake.

4. Ask yourself whether this even makes sense at all

An extremely popular phishing attack that's been employed for years and is still used today is when a cybercriminal reaches out to an unsuspecting victim, usually by email, with a promise that they have millions of dollars to give the potential victim for no real reason at all. If the unsuspecting victim just clicks on a link, then the hacker can infiltrate their computer.

I always tell people, when you see something like this, ask yourself, "Does it make any sense at all?" No one you don't know is going to give you millions of dollars for no real reason — and chances are, no one you do know will give you that kind of money either. This advice applies not only to spotting phishing attacks, but also fake news. The next time you read or watch something that sounds so unbelievable you just have to share it with your network, take a

second and follow some of the other recommendations in this article before helping spread the possible fake news. This way you can be part of the solution rather than adding to the problem.

The digital world gives us access to a wealth of knowledge, allowing us to carry entire libraries in the palms of our hands. But it also gives us access to criminals, spammers, fake newsmakers, trolls and a wide range of other nefarious people looking to deceive us. When the age of information becomes an onslaught of misinformation, it's up to us to be aware of what is real and what is fake. Take your time, and do your research. Think with logic instead of emotion. And stay informed, aware and safe.

By Danny Pehar