The Expert's Opinion on Protecting Yourself From Cyber Attacks

Paige Hanson

Scams really have two different derivatives. There's the first one, which is the "too good to be true" message. Whether you're going to win a car, a sum of money, maybe you get a new promotion, whatever it is, it's too good to be true.

And then, you have on the other side, the fear-based message. You're locked out of your account, and you're losing money, or something's happened to a loved one.

If you can remember those two things, in order to recognize scams, you'll be safer. It is a fear-based message or a "too good to be true" message because they want you to react. Ongoing training within your organization will help users identify those types of emails.

There's also different protocols and training systems that you can put in place to make sure that your employees when they see a suspicious email, link, or attachment, they know to forward that to your IT or your credible organization that will help them determine whether or not that actually is a fraudulent email.

Ransomware is tough. It can be as little as saying "We have a handful of your files. Pay us $X amount." Or they could have all of your files and say that they're going to exploit all of your customers information. So that can be a very scary situation for any business.

You definitely want to make sure you're connecting with law enforcement and getting their feedback to see if there's a further investigation.

But first and foremost, you want to make sure that there is ongoing training within your corporate daily life because a lot of times you are as weak as your weakest employee.

All a fraudster needs is for your employees to respond to one email, click on one link. So if you have ongoing training – proactive training – within your company dynamic, that'll definitely make you safer.

Amerifund