THE REAL CYBER RISKS

BY JAY BORDEN

We all hear about companies and organizations being hacked resulting in our private information being exposed. Sadly, this occurs so often we are getting numb to it and feel there is nothing we can do. So why worry?

But there is good reason to be concerned. Our information can be used for many nefarious purposes, make purchase on your credit cards, drain your bank account, steal your identity, pressure you to reveal confidential information about your employer, and more.

As with any situation, before you can determine what to do, it is important to understand it first. Then find ways to be safer.

The news about the breaches and compromises of our information typically put the blame on cyber hackers and criminals. These groups do exist and do much damage.

However, it is important to understand that most of the breaches are not due to hacking or breaking in to systems. The main cause is people clicking a bad link, falling for a phishing email, or otherwise making errors. Doing these things puts your credentials into the hands of the attackers. Research puts people as the cause of 80% or more of breaches, with some estimates as high as 95%.

The attackers are very good at sending messages and emails that appear real or appear to come from a trusted party. Not surprising that we fall for them. Especially when we are all so busy it is difficult to find the time to analyze and check things to determine if they are what they appear to be. Did that email really come from an executive at your company? Or your bank? Or the IRS? Or any other source we would trust?

THE REAL CYBER RISKS

CONTINUED

Artificial Intelligence, AI, is helping attackers craft messages that are even more convincing.

How are these messages delivered? Phishing is the most common way and come as emails that appear to be from a trusted party such as a bank, company executive, government agency, etc.

A variation is called vishing and uses phones and voicemail to deliver the fake messages. AI systems only need a few words of someone's voice to make the it appear the real person is saying anything they want. The snippets can be from a speech the person made, a keynote they gave, a phone call, or other sources.

One more variant is called smishing and uses text messages to deliver the fake messages and links.

The challenge is that anti-malware programs may not detect anything wrong with these messages. Certainly not with a voicemail message. As anti-malware gets better at examining the links to see if the sites are corrupt, the attackers get more creative. The destination site may not have malware so it passes the tests, but redirects to another site to get your information. The antimalware may not see the redirected site

Other ways our information gets compromised is when we willingly give our private information, but it is also captured by a someone for nefarious purposes. For example, how many times are we asked for our email address to receive a receipt for a purchase? Maybe it's in a store or a coffee shop. But if anyone overhears you, they also have your email address. If the store gets hacked, your email address is gone.

Attackers are very good at combining bits of seemingly innocent information to get enough to send a convincing message. For instance, you just gave the store your email. Attackers capured it and know what store you are in and can see what you purchased. If you received an email that appeared to come from that store saying your credit card for the purchase of the named item didn't go through. Please click the link in the email and re-enter your credit card number. Very believable isn't it? Would you click the link? Now the attackers have just convinced you to surrender your credit card information.

THE REAL CYBER RISKS

CONTINUED

Another tactic is to send an email that appears to be from that store asking you to fill out a survey about your experience. To do that you will have to prove your identity. Sounds reasonable. But again, more personal information ends up with attackers. Or the survey asks seemingly innocent questions. But gathers more information about you.

Have you heard of shoulder surfing? It is someone standing close enough to observe what you do on your phone. Think about it. You check email, your bank balance, make a purchase, etc. If someone is standing close enough they can capture enough information for a successful attack.

Public WiFi is another risk. It is never well protected, and a savvy attacker can capture your traffic, email passwords, bank account information, etc. You get the picture.

What to do?
Take the time to verify if those emails, voice mails, or texts are from the apparent sender. Never click a link in them or reply to them. Use a communication method you have used before. Such as a known phone number or one found on the company's website.

Do not use your phone or computer on public WiFi. That may be inconvenient, but not as inconvenient as having to reclaim your money or identity. Use the cell network.

Never use your phone where someone can shoulder surf and see your phone. Do not assume the person standing that close is innocent. This is not paranoia, just being smart in today's environment.

The old saying about an ounce of prevention is better than a pound of cure is applicable here.

Be sensible and protect your information.

Visit our site, onebrightlycyber.com to learn all the ways we help keep you safer.

Welcome to peace of mind.