nerej
CELEBRATING 55 YEARS

Cybersecurity threats that we must understand and work to prevent - by Dawn Pereyo

June 19, 2020 - Spotlights

Dawn Pereyo
Westcor Land Title Insurance Co.

With all the evolving technology that we use while conducting our business day-to-day, there are also inherent risks that we now must face head on. Online scams, phishing emails, and security breaches are just some of the cybersecurity threats that we must understand and work to prevent. One of the most common cyberthreats we face is phishing emails, and the damage that could potentially come along with it such as wire fraud.

According to the FBI, phishing “is the act of sending an e-mail falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers and bank account information.” The emails can seem friendly, even sound personable and seemingly come from an email address that you recognize. However, they can lead to wire fraud, and while working in an industry that handles customers personal data, the implications of just clicking an average-looking link could be catastrophic.

How catastrophic can a cyberattack get? From 2013 to 2016, cyber-attacks cost businesses over $5 billion worldwide, from 2016 to 2017 phishing attacks increased by 65%, and by 2018, 83% of people received a phishing attack, according to the American Land Title Association. Phishing attacks are not just a data security problem but can lead to millions of dollars in damages.

What can I do to prevent it? To insure you’re not falling into a phishing scam, make sure to check the following, as they might be a tell-tale sign that this email is coming from a scammer:

• Check the email address: Sometimes scammers will make email addresses extremely similar to one from a bank or lender in hopes of you just assuming that it is who it says it’s from.

• Don’t provide personal data: Never share your own personal data or your customers data without an encryption, as emails if not originally involved in a phishing scam can be used indirectly in an attempt on someone else.

• Verify, verify, verify: This is especially important when we refer to wire transactions or requests. Make sure to either call the person requesting this action to double check it’s legitimate. Always confirm the information.

• Anti-Virus Software: Make sure your computer is running anti-virus software so that in case malware, a virus coming from clicking a link in a phishing email, can be located and stopped as soon as possible to prevent further damage to you, your company and your customer’s data.

What do I do if I think I’ve been scammed?

• Report the phishing email to your internal IT department or IT vendor immediately and follow all instructions they provide to you regarding the further use of your computer, email, etc.

• If you have discovered you are a victim of a wire fraud scam, file a complaint with the FBI at www.ic3.gov.

While there are these inherent risks, technology has helped our industry continue to grow and expand its capabilities. Being proactive and learning about potential threats to our data can lead us to even more prosperous relationships with customers who feel safe working with us.

Dawn Pereyo is vice president and northeast region manager for Westcor Land Title Insurance Company, Melville, NY.