Don't Get Reeled into a Phishing Scam

In an increasingly connected world, businesses are able to work more effectively and efficiently than ever before — but they are also more susceptible to fraud than ever before. It might seem impossible that your business would be the target of a digital scam, but that's what cybercriminals are counting on. They prey upon the unsuspecting, employing ever-evolving methods to gain access data they can exploit for profit.

According to the FBI's Internet Crime Complaint Center, nearly 70,000 U.S. businesses lost more than $10.1 billion to business email compromise/email account compromise attacks, commonly known as phishing, between October 2013 and July 2019[1].

Phishing attacks happen to businesses of all sizes and types. Scammers will send emails to employees, asking for information or providing a link that, when clicked, gives them access to the business's network. From there, the criminals can install malicious software to extract information, hold data for ransom, or otherwise sabotage a network.

One thing all phishing attacks have in common is that an employee was deceived — either into following a link, paying money, or providing information to someone posing as a trusted source. So, what can you do to help prevent your business from being reeled in by such a scam? Learn about the problem, then educate your employees. Here are a few tips to help get your workers thinking about helping protect your data — and your business — from email scams:

- Generic greetings, misspellings, and sloppy presentation could signify that an email is fraudulent
- If an email requests payment, but you weren't expecting an invoice, confirm it with your known contact over the phone
- If an email contains an unfamiliar or suspicious link, don't click it
- Report all suspected email attacks to management, but don't forward emails unless requested

Any organization is vulnerable to phishing attacks. So take steps to mitigate your risk of being a victim. Consider investing in cyber liability insurance to help your business respond to cyber exposures. Keep your systems and software up to date. Teach your employees to guard against cyber scammers. Consider hiring a vendor that specializes in analyzing your susceptibility and training employees to recognize and avoid malicious emails.

This threat is not going anywhere; fraudsters continue to find new ways to catch their victims off guard. But understanding the risk and training your employees to help safeguard your data and your network is the best first step you can take to help keep your business from falling victim to cybercriminals.

[1]*Source: "Business Email Compromise: The $26 Billion Scam." https://www.ic3.gov/Media/Y2019/PSA190910. Accessed November 2020.*