PPP-Related Scams To Avoid

cyber security pandemic phishing

Summary: The PPP brought much-needed funds to many businesses. Yet, it has also brought fresh fraud opportunities. We highlight the three latest cybersecurity scams connected with PPP to protect you and your customers.

Remember the movie, "The Terminator"? This sci-fi thriller set in 2029 came out in 1984 and was #1 at the box office with $4MM in gross revenue. Wouldn't it be nice if we could terminate cyber thieves? They just keep showing up and wreaking havoc.

In the face of the pandemic, fraudsters have found a fresh opportunity to prey on the confusion and concern of average bank customers to gain access to privileged information and accounts.

Many of these scams are connected loosely to the Paycheck Protection Program (PPP), so CFIs should take note. The financial scams that people and businesses need to avoid include:

Email attachments. This is still the most basic and common online access to data. Many bank customers, consumers, and small business owners alike, may receive a seemingly innocuous email, saying that it offers information or details connected to the PPP program. However, like so many other scams, these emails often carry a fraudulent link that connects customers to a hacker website or downloads a virus. Be sure to educate your PPP customers on the dangers of these types of emails.

Web pages. The Cybersecurity and Infrastructure Security Agency has issued a warning regarding at least one cyber thief who is spoofing the Small Business Administration COVID-19 relief webpage through phishing emails. The phishing emails contain a malicious link to a fake page used for re-directs and credential stealing. The phishing email subject line currently reads, "SBA Application - Review and Proceed" and the sender is marked as "disastercustomerservice@sba[.]gov". In general, these links can appear very legitimate, which serves to lure in unsuspecting and well-meaning bank customers. But on closer look, the extra characters in the domain can increase your suspicion.

Phishing schemes. Look out for phishing attacks/scams utilizing the SBA logo. In many cases, these fraudulent links will lead bank customers to input their personally identifiable information (PII), to obtain personal banking access, or to install ransomware or other kinds of malware on a customer's computer. Any email communication from SBA will come from accounts ending with sba.gov. The presence of an SBA logo on a webpage does not guarantee the information is accurate or endorsed by SBA. Cross-reference any information you receive with information available at www.sba.gov or encourage your customers to visit the SBA website and log in instead of using the links found in the email.

Unfortunately, hackers stepped up their game because of the amount of money flowing through the PPP. The scams are similar to those we have seen before. But, when times are tough, decisions are sometimes made in haste. Keep reminding your team and your employees to stay strong while sharing and re-sharing tips with your customers!

LOAN GROWTH AND FLOATING RATE ASSETS

Your institution can purchase fully-funded, senior secured floating-rate loans to diversify your portfolio. Contact us today for more information.