Tips To Stop Stressing About Payroll Phishing

cyber security risk management human resources

Summary: Payroll phishing scams are on the rise. What your bank can do to protect itself and its employees.

A study on mobile phone usage finds running out of phone battery at a crucial time can be more stressful than running late to work or going to a job interview. People seem to feel more isolated or unable to perform to their capabilities without a working phone.

No matter what stresses you out, Intermedia's 2017 Data Vulnerability Report finds roughly 20% of office workers certainly have been stressed due to becoming a victim of a phishing email. These types of attacks are on the rise, so banks need to know what to look for and how to respond.

One recent phishing scam targets a company's payroll. There are several versions of this scam, but the upshot is that thieves are using information they obtain from employees to access payroll and steal paychecks.

Law firm Ogletree, Deakins, Nash, Smoak & Stewart lays out one possible scenario. The scam begins with an employee receiving an email that appears to come from within his or her company. It might be an e-signature request or a survey response request. Employees are directed to click a link, access a website or possibly answer a few questions. Then, employees are asked to confirm their identity by providing their log-in credentials. Once thieves have this information, they can cause all sorts of havoc by accessing payroll portals, rerouting direct deposits to other accounts and more.

The thieves are clever in their efforts and have even come up with a workaround for skeptical employees who attempt to determine their legitimacy by responding to the sender. Those who try this route receive a prompt response "verifying" that the employee should follow the link's instructions.

One of the major problems with phishing emails is that they seem authentic and even savvy employees familiar with the idea of phishing attempts can easily be duped. We can't stress enough the need to familiarize employees about these types of scams and proactively train them how to react when there are doubts about an email's legitimacy. Here are some concrete things banks can do to help prevent harm:

EDUCATE: This may seem obvious, but it is nonetheless important. Be sure to remind employees frequently never to click on an unfamiliar link in an email, even if it seems legitimate. If employees have any questions, they should pick up the phone and call human resources or the IT department. Employees should never hit reply to one of these emails or call a phone number given in the email.

TEST AND TRAIN: A number of banks regularly send their own version of phishing emails to staff members. The logic is simple. Any employee who takes the bait and clicks on the link receives extra training. Banks reason that it's better to be proactive than to risk employees inadvertently clicking on a real scam. If you are trying this approach, the trick is to make the phishing emails seem believable. The reason so many people are ensnared by phishing emails is that they are highly believable. If you make your test messages obviously fake, you're wasting your time.

REMIND: It's important to remind employees frequently that you will never ask them to share passwords or provide sensitive information over email. Repeat this message often and hopefully it will cause everyone to think twice.

As phishing scams get more and more sophisticated, it becomes even more incumbent on banks to be proactive. Like losing your phone battery at a bad time, phishing emails can leave you feeling isolated or unable to perform work, because they can be very damaging and have long-lasting consequences for employees and the bank.

DEPOSIT OPPORTUNITIES

In an effort to expand our relationships, PCBB is pleased to offer community banks a money market deposit account rate of 1.85%, subject to availability. Contact operations@pcbb.com.