BANC OF CALIFORNIA | TOGETHER WE WIN®

YOU CAN BANC ON IT
QUESTIONS WE NEVER ASK

WHY DO EMPLOYEES GET CAUGHT IN PHISHING?

Lack of training might be part of it, but there are other factors that make employees vulnerable.

There's a term used in cybersecurity that business owners and their employees need to know—phishing. It's a particular type of scam that's been getting a lot of attention the past five years or so.

Every year, thousands of employees are fooled into divulging valuable company information (and secrets) to people they believe to be colleagues, bosses or vendors. Sometimes, the employees are asked to make a wire transfer, which they do willingly. As it turns out, those people making the request are actually con artists...cyberthieves.

Businesses lose millions of dollars to phishing annually. It's estimated that phishing is also responsible for more than 75% of data breaches. The amount of money lost to cybercriminals more than tripled from 2015 to 2019. Cybercrime affects companies of all sizes in all industries, all over the world. It's a serious problem that's not going away anytime soon.

Awareness is an important component in the fight against phishing.

Despite all the awareness phishing has gotten, it still works well for scammers, even if employees have heard about it. There has to be more than meets the eye.

Why do employees fall for scams?

In the same way a car accident can happen no matter how alert and careful a driver is, a phishing incident can happen in the same way, without an employee being reckless, careless or negligent.

Here are some scenarios that might make one of your employees vulnerable to a scam:

A new employee. Someone who's been on the job a short time is a prime target and has a high likelihood of being fooled and victimized.

A busy or overtasked employee. Many companies have had staffing issues due to the pandemic. Many employees are wearing multiple hats and are busier than ever, which means they could be caught with their guard down.

An employee who's eager to help or please. A staffer who thinks they're going the extra mile or saving the day could be making a scammer quite happy by inadvertently cooperating.

A naive or trusting employee. Even training to discern and prevent phishing might not help here. Some on your staff might have a kind and gentle nature, which is good for the workplace... but not good for catching a phishing attack in progress.

Employees of a company at all levels are potential scam targets...but that doesn't mean they'll be scam victims. They can avoid traps by keeping their eyes open and their scam radar on high.

SPOT THE RED FLAGS. AVOID A SCAM.

An employee who feels isolated. Employees who have little interaction with others could become detached from their company's goals and mission. They may simply follow any request as part of getting through their day.

An employee handling new duties. If an employee has been promoted or is being cross-trained, they may be susceptible to a sudden request or demand they receive.

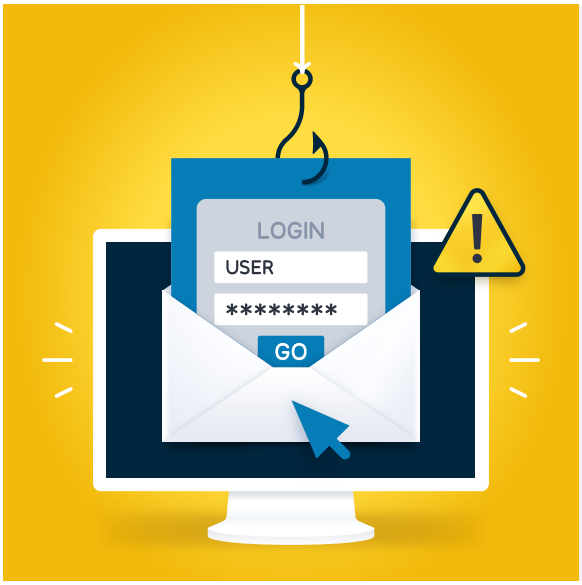
The truth is there are many reasons a phishing scheme could work on any random day...if the scammer and his phishing bait come in at the right time to the right employee.

How to protect your employees and your business.

Phishing attempts and other scammer efforts will be around for a long time. Employees will come and go, even some of the best-trained ones, which is why it is vital for businesses to establish an anti-fraud campaign that not only teaches employees about the variety of scams, how they work and what to look for, but also focuses on the target of the scams: your employees.

Cybersecurity experts have this advice for companies: Train everyone. Train often. And keep cybersecurity awareness high.

Your employees are important to your success, but they're only human. With the right training, support and sense of appreciation for what they do, they'll learn to perform their roles well while keeping an eye out for scammers and fraudsters who could be ready to attack.



Some job functions are prime targets for "spear phishing" scams.

In many instances, a scammer will target a business's employees by gaining information on them through social media and other research. They'll find out their name and title and determine if they might have authority to authorize transactions. They'll also target employees who might have access to key information, such as codes to networks or even the names of other employees in a targeted department.

If you believe that an employee in a sensitive position might fall into one of the above categories, you'll see how or why a phishing attack might work in spite of your company's best efforts.

To read more Business Insights articles, please visit: **bancofcal.com/business-insights**