BANC OF CALIFORNIA | TOGETHER WE WIN®

YOU CAN BANC ON IT

QUESTIONS WE NEVER ASK

SPOT THE RED FLAGS. AVOID A SCAM.

It's sad to say, but by now consumers and business owners are used to hearing the same news, year after year, month after month: **Scams are on the rise and they're not going away anytime soon.**

The statistics prove it. According to the Federal Trade Commission, 5.7 million people filed fraud reports, and that led to an estimated $6 billion in losses. Those numbers are up about one-third from the year before.

On the business side of things, the news is just as discouraging: About 80% of organizations have experienced social media "phishing" attacks.

However, there is some good news despite the gloomy statistics. According to research about how scams work, awareness of them drastically reduces the chances of people being fooled.

Looking out for the "red flags."

In our everyday lives, we know that a red flag can literally be a sign of trouble ahead. On a highway, it means there's a hazard. A red flag on a beach means don't go in.

As it turns out, scams have their own red flags. Why? Because the words a scammer uses, the requests they make and how they make them are typically out of the norm and can give them away. When a consumer spots a red flag in a text, email or phone call, they can disengage from the conversation.

That's especially relevant for business banking and for the banking industry because con artists regularly attempt to fool employees by pretending to be an employee of a bank.

A simple "wait a minute..." and disruption to the scheme by the target of a scam can eliminate the chance of it working.

If a company's employees learn to recognize the signs of a phishing attempt or other scams, they greatly increase the chances of deterring and avoiding them. In other words, if you can recognize and learn the red flags that indicate a possible scam, the chance of avoiding one is extremely high.

"You want me to do what?"

Here's a rule of thumb that can be helpful to remember and should be passed along to your employees: If your bank asks you to do something completely out of the ordinary that you've never done before, there's a good chance it's not really your bank that's doing the asking.

"A good habit to develop to avoid a scam is not to respond immediately to an important request. Pause before acting. Scammers create a great sense of urgency to get you to do something without thinking it through or checking it out."

Mike Krueger
Senior Vice President, Chief Information Security Officer, Banc of California

SPOT THE RED FLAGS. AVOID A SCAM.

The red flags that can alert you to a scam!

Whenever you get a message from Banc of California (or another company you deal with), examine the essence and content of the message.

Scammers have a different agenda from the people they're impersonating, so they often give themselves away.

More than that, they're hoping to hook the easy catches. If you examine their communications, you might spot the scam quickly and stop it in its tracks.

Here's what to look for:

Sloppy communications: Read the texts and emails closely. Often, a scammer's message will contain:

- Incorrect grammar
- Unprofessional language
- Multiple typos

Of course, if the scammer is more sophisticated and their native language is the same as yours, that might not be the case.

Unusually harsh messages: Bullying tactics are used often by scammers.

- High-pressure language
- Scare tactics, such as the threat of suspending your account
- A sense of great urgency
- Threats of law enforcement action

Can you imagine any professional bank using these tactics? If a caller goes down this path, disengage immediately from the conversation.

Account-specific questions: Requests of this kind are a clear giveaway.

- For sensitive account info
- For passwords or your Social Security number
- For your PIN or a login code that's texted to you

In the previous article in this series, we listed the many questions and types of information we will never ask you in an email, text or phone call.

Untypical requests: Lastly, a cybercrook might simply cut to the chase in their message and make a simple request of you, without all the fuss. These tactics also work more than they should.

- To visit an unfamiliar, unrelated website via a suspicious link
- To call a phone number different from the one listed on your card
- To send money via wire transfer or Zelle®
- To click on attachments in an email

A few seconds can save you a world of headaches.

Because scammers are relentless, it's important to follow this advice: Take your time to carefully read any messages you receive, and wait a few seconds before you decide to continue and respond.

*Source: money.com/money-scams-spike-2021

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

BANC OF CALIFORNIA | TOGETHER WE WIN®