BANC OF CALIFORNIA | TOGETHER WE WIN®

HOW TO SPOT THE WARNING SIGNS OF THE MOST COMMON PHISHING SCAMS

Businesses are a favorite target for phishing scams, where con artists impersonate a trustworthy figure, like someone from your bank.

Mobile payment phishing signs

They suggest using a payment app (PayPal®, Venmo®, Zelle®, etc.) to settle an overdue payment or open a new account. They give you the option of making a mobile payment to yourself to prevent a fraudulent transaction.

Email phishing signs

Suspicious links that could be harmful; scare tactics, threats, pressure to comply from the email sender; typos and nonprofessional language and approach in the email.

Phone call phishing signs

A high sense of urgency; request for sensitive account details; caller ID “seems” correct (but can’t be trusted); getting an unexpected call from your bank...why?

Text phishing signs

A demand for a quick response; threats and high-pressure messages; request for account or personal information; embedded links to click.

QUESTIONS WE WILL NEVER ASK: YOU CAN BANC ON IT.

There are questions that Banc of California would never ask you, specifically regarding passcodes or personal identifiable information, nor would we pressure you to use a mobile payment app or make a fast decision.

Our goal is to help our clients succeed by providing customer solutions and unparalleled, personalized service. At the same time, we help you protect what you’ve built by providing timely information regarding cybersecurity.

That’s the Banc of California Difference.

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

Click the link below for an in-depth look at this topic and to read the full article