## Can You Spot a Phishing Scam?

Every day, thousands of people fall victim to fraudulent emails, texts and calls from scammers pretending to be their bank. And in this time of expanded use of online and mobile banking, the problem is only growing worse. In fact, the Federal Trade Commission's report on fraud estimates that American consumers lost a staggering $5.8 billion to phishing scams and other fraud in 2021—an increase of more than 70 percent over 2020.

It's time to put scammers in their place.

Online scams aren't so scary when you know what to look for. And at Harvest Bank, we're committed to helping you spot them as an extra layer of protection for your account. We've joined with the American Bankers Association and banks across the country in a nationwide effort to fight phishing—one scam at a time.

We want every bank customer to become a pro at spotting a phishing scam—and stop bank impostors in their tracks. It starts with these four words: *Banks Never Ask That*. Because when you know something sounds suspicious, you'll be less likely to be fooled.

These four phishing scams are full of red flags:

- **Text Message**: If you receive a text message from someone claiming to be your bank asking you to sign in, or offer up your personal information, it's a scam. **Banks Never Ask That**.

- **Email**: Watch out for emails that ask you to click a suspicious link, download an attachment or provide personal information. Links in phishing messages may direct you to fraudulent websites. Attachments can contain malware such as viruses, worms or spyware. Ignore any requests from the sender, do not reply to them, and do not call any phone numbers provided in the message. The sender may claim to be someone from your bank, but it's a scam. **Banks Never Ask That**.

- **Phone Call**: Would your bank ever call you to verify your account number? No! Never give personal information to the incoming caller. Be aware that area codes can be misleading. If your Caller ID displays a local area code, this does not guarantee that the caller is local. If you're ever in doubt that the caller is legitimate, just hang up and call the bank directly at a number you trust. **Banks Never Ask That**.

- **Payment Apps**: Beware of text messages from someone claiming to be your bank saying your account has been hacked. The scammer may ask you to send money to a new account they've created for you, but that's a scam! **Banks Never Ask That**.

If you feel you've been the victim of a scam and may have provided personal or important financial information, contact Harvest Bank immediately. Be sure to include any relevant details, such as whether the suspicious caller attempted to impersonate your bank and whether any personal or financial information was provided to the suspicious caller.

You've probably seen some of these scams before. But that doesn't stop a scammer from trying. For tips, videos and an interactive game to help you keep phishing criminals at bay, visit **www.BanksNeverAskThat.com**. And be sure to share the webpage with your friends and family.

HARVEST BANK