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 banking, the problem is only growing worse. It's time to put scammers in their place.

Online scams aren't so scary when you know what to look for. And at HVB, 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 what sounds suspicious, you'll be less likely to be fooled.

These top 3 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 or provide personal information. The sender may claim to be someone from you bank, but it's a scam. Banks never ask that.
- Phone Call: Would your bank ever call you to verify your account number. No! Banks never ask that. If you're ever in doubt that the caller is legitimate, just hang up and call the bank directly at a number you trust.

For tips on how to keep phishing criminals at bay, including videos, an interactive quiz and more, visit **www.BanksNeverAskThat.com**.

HVB
The better experience BANK

Member FDIC