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.

Online scams aren't so scary when you know what to look for. Banks are committed to helping you spot them as an extra layer of protection for your account.

We want bank customers to become pros 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 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! **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.

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

What's Your Scam Score? Take five minutes to become a scamspotter pro by taking the #BanksNeverAskThat quiz at www.BanksNeverAskThat.com. Share your score with your friends and family and encourage them to test their scam savviness, too. The more scamspotters out there, the harder it is for phishing criminals to catch their next victim!