Ever received an email asking for your bank account number? It's probably a scam, because #BanksNeverAskThat. See what else banks never ask—and test your scam IQ ▼

Have you ever received an urgent text message, one that claimed to be from your bank, that asked you to call them at a new number? It's probably a scam, `cause #BanksNeverAskThat. Test your scam IQ ▼

Go to **BanksNeverAskThat.com** and take the **#BanksNeverAskThat quiz**

Have you ever received an email that appeared to be from your bank, but it asked you to click a suspicious link? Nice try, scammer. #BanksNeverAskThat. See what else banks never ask—and test your scam IQ ▼

Would your bank call you to verify your password? Nope. #BanksNeverAskThat. Just hang up, and call the number on the back of your card. Take this quiz to find out if you're an expert scam spotter ▼

Go to **BanksNeverAskThat.com** and take the **#BanksNeverAskThat quiz**

We all get spammy texts. But what if it looks and sounds like your bank? Here's one way to tell it's a scam: it asks you to click a link. #BanksNeverAskThat. See what else banks never ask—and test your scam IQ ▼

Would your bank call you to verify your account number? Nope. #BanksNeverAskThat. Just hang up, and call the number on the back of your card. Get more tips, and take the quiz, here ▼

Go to **BanksNeverAskThat.com** and take the **#BanksNeverAskThat quiz**

#BANKSNEVERASKTHAT TALKING POINTS

Phishing scams are taking a toll on consumers, including bank customers.

- Every day, thousands of people fall for fraudulent emails, texts, and calls from scammers pretending to be a bank. These are commonly referred to as phishing scams. The communication is designed to trick you into providing confidential information (like account numbers, passwords, PINs, or birthdays) either online or over the phone to someone imitating a bank employee.

- Victims of phishing scams can lose hundreds, even thousands of dollars. The FTC estimates that consumers lost $1.48 billion to phishing schemes in 2018 and the pandemic has only increased the threat.

- Scammers are taking advantage of the fear and uncertainty surrounding COVID-19, as well as the expanded use of digital banking platforms, and tricking consumers into giving up their personal and financial information.

Education is the key to preventing these types of scams.

- Educating our customers is one of the most effective ways to prevent them from falling victim to these scams.

- We are joining banks across the country to raise awareness about phishing scams and help customers think twice before clicking a link or giving up personal information by email, text or over the phone.

To spot phishing scams, just remember "Banks Never Ask That."

- If you receive an email, text, or phone call asking for confidential information, it's a definite red flag. It's better to be safe than sorry. End the call, delete the text, and trash the email, because banks never ask that!
  You may be asked to verify confidential information if you call your bank, but never the other way around. If you receive an incoming call from someone claiming to be your bank, the safest thing you can do is hang up and call your bank's customer service number.

The #BanksNeverAskThat campaign seeks to turn the table on fraudsters by empowering consumers to spot bogus bank phishing scams.

- Consumers can visit BanksNeverAskThat.com to take a phishing quiz and to learn more about phishing scams. There are also social media posts that they can share with their family and friends to help spread the word.

ADDITIONAL CONSUMER TIPS

If you receive a suspicious email or text:

- Do not download any attachments in the message. Attachments may contain malware such as viruses, worms or spyware.

Please continue to Page 2 for more tips.

#BANKSNEVERASKTHAT TALKING POINTS

- Do not click links that appear in the message. Links in phishing messages direct you to fraudulent websites.

- Do not reply to the sender. Ignore any requests from the sender and do not call any phone numbers provided in the message.

- Report it. Help fight scammers by reporting them. Forward suspected phishing emails to the Anti-Phishing Working Group at reportphishing@apwg.org. If you got a phishing text message, forward it to SPAM (7726). Then, report the phishing attack to the FTC at ftc.gov/complaint.

If you receive a suspicious phone call:

- If you receive a phone call that seems to be a phishing attempt hang up or end the call. 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.

- Do not respond to the caller's requests. Financial institutions and legitimate companies will never call you to request your personal information. Never give personal information to the incoming caller.

If you feel you've been the victim of a scam and may have provided personal or important financial information, contact your bank immediately at their publicly listed customer service number. Often, this is found on the back of your bank card. 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.

BEO Customer Service: 541-676-0201 or Contact your Local Branch.