#BANKSNEVERASKTHAT

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 $3.3 billion to phishing schemes and other fraud in 2020.

- 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.

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.

- (SEE ADDITIONAL CONSUMER TIPS BELOW.)

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.

- 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.