Don’t fall for fake. Keep your money safe by learning the red flags of phishing.

Brought to you by

American Bankers Association®

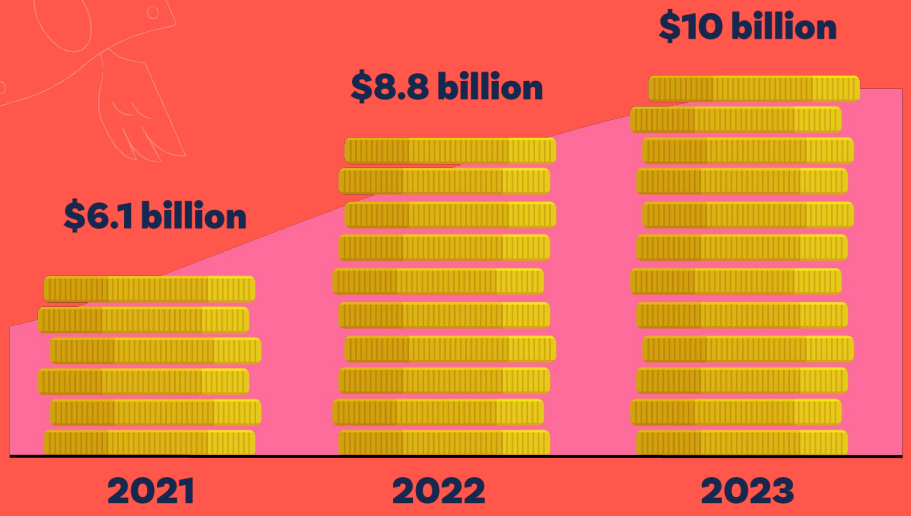
ADD BANK LOGO HERE

Every day, people fall victim to fraudulent emails, texts, calls, and payment app requests from scammers pretending to be their bank.

That's phishing.

BANKS NEVER ASK THAT .com

ADD BANK LOGO HERE



How bad is it?

Consumers lost over $10 billion from phishing and other scams in 2023 — a 13.6% increase since 2022.

BANKS NEVER ASK THAT

ADD BANK LOGO HERE

So what can you do?

1. Learn to spot the red flags of phishing scams.
2. Defend your accounts against future threats.
3. Take action if you think you've been a victim to a scam.

BANKS NEVER ASK THAT

ADD BANK LOGO HERE

1

Learn to spot the red flags of phishing scams.

BANKS NEVER ASK THAT

ADD BANK LOGO HERE

The red flags of…

Phishing Emails

Watch for these red flags:

1. Suspicious email address
2. Typos or unusual grammar
3. Urgent language
4. Hyperlinks — never click them
5. Attachments — never open them

URGENT: Account activity alert

info@pinecreek-bank-us.co 1

Dear Customer

We received a mobile request from you, or someone with access to your account, to make changes ot your Pine Creek Online bank Profile.

If you did not authorize thes changges, please varify our 2 account with your account PIN or Social Security Number through the link below!

Sign On below to verify your account dettails. Note that entering incorrect account information will result in your account being closed IMMEDIALTELY! **ACT NOW!** 3

Verify your PIN or SSN
https://www.pinecreek-bank-us-co/log-in 4

or view your account transactions attached

5

ao830xhb33nr...

BANKS NEVER ASK THAT

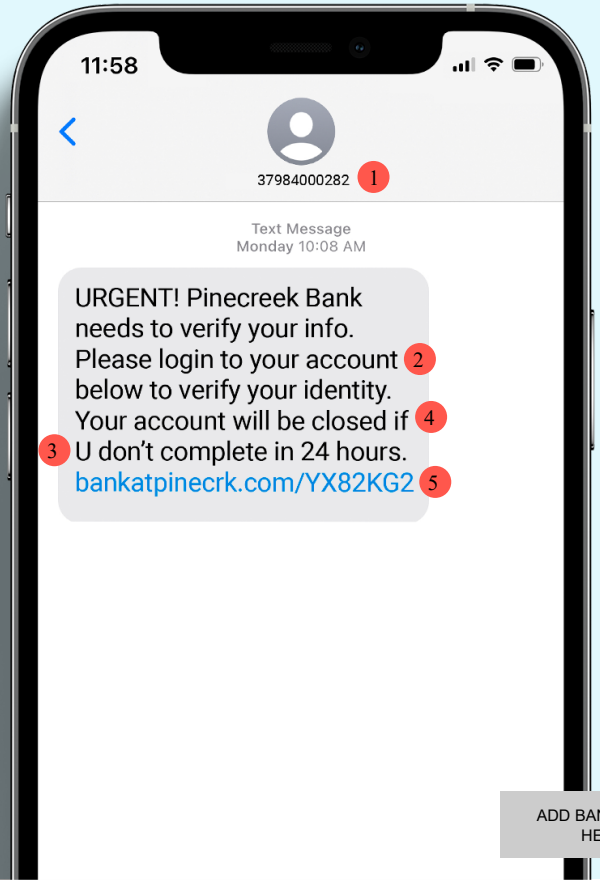
ADD BANK LOGO HERE

The red flags of…

Phishing Texts

Watch for these red flags:

1. Unusual phone numbers —your bank will only text from a 4-5 digit number
2. Hyperlinks — your bank will never ask you to log into your account by texting a link
3. Odd grammar
4. Scare tactics and urgent language
5. Texts asking you to open a link



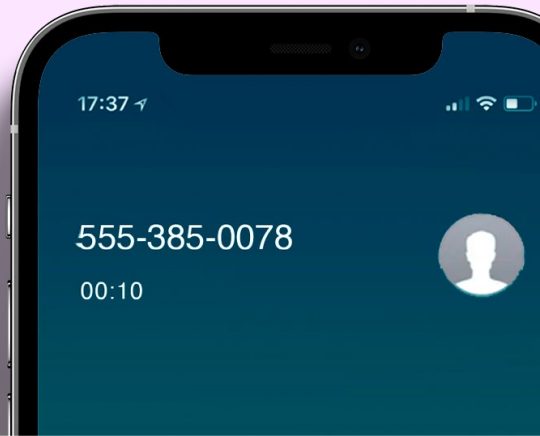
BANKS NEVER ASK THAT

ADD BANK LOGO HERE

The red flags of…

Phone Call Scams

"Hi, I'm calling to notify you that your credit card was breached. Before we begin, can you please verify your identity with your name, address and card number?"



Stay safe with these tips:

- Watch out for a false sense of urgency
- Never give sensitive information
- Don't rely on caller ID

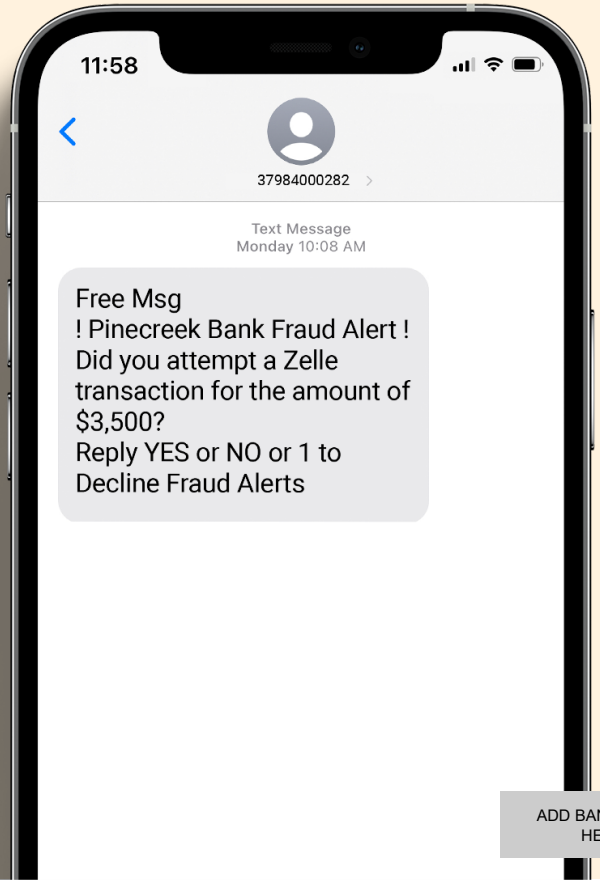
BANKS NEVER ASK THAT

The red flags of…

Payment App Scams

Stay safe with these tips:

- Be wary of texts or calls about payment apps
- Use payment apps to pay friends and family only
- Raise the alarm on urgent payment requests
- Avoid unusual payment methods



BANKS NEVER ASK THAT

ADD BANK LOGO HERE

2

Beef up your defenses.

BANKS NEVER ASK THAT

ADD BANK LOGO HERE

Lock down your accounts

#1
MFA

Set up multi - factor authentication on your bank and email login.

#2
Strong Passwords

Use random or complex passwords.

#3
Updated browsers

Keep your browsers up-to-date with the latest defenses.

#4
Use antivirus

Use defenses like virus protection and malware alerts.

ADD BANK LOGO HERE

3

Got scammed? Take action.

BANKS NEVER ASK THAT

ADD BANK LOGO HERE

If you believe you've been scammed, take these next steps:

Step #1

Contact your bank.

Step #2

Change your passwords and visit IdentityTheft.gov.

Step #3

Report the scam to the FTC at ReportFraud.ftc.gov.

Step #4

If you lost money, file a police report.

Learn more with these links:

- BanksNeverAskThat.com
- <<<bank website>>>

ADD BANK LOGO HERE