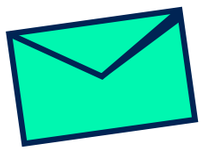
Phishing Scam Tips

Every day, regular people like you lose their hard-earned money to online phishing scams. Don't fall for fake — learn how to spot shady texts, emails, and phone calls by knowing the things your bank would never ask.

BANKS NEVER ASK THAT .com



Email Scams

Email scams account for 96 percent of all phishing attacks, making email the most popular tool for the bad guys. Often, the scammer will disguise the email to look and sound like it's from your bank.

Avoid clicking suspicious links

If an email pressures you to click a link — whether it's to verify your login credentials or make a payment, you can be sure it's a scam. Banks never ask you to do that. It's best to avoid clicking links in an email. Before you click, hover over the link to reveal where it really leads. When in doubt, call your bank directly, or visit their website by typing the URL directly into your browser.

Raise the red flag on scare tactics

Banks will never use scare tactics, threats, or high-pressure language to get you to act quickly, but scammers will. Demands for urgent action should put you on high alert. No matter how authentic an email may appear, never reply with personal information like your password, PIN, or social security number.

Be skeptical of every email

In the same way defensive driving prevents car accidents, always treating incoming email as a potential risk will protect you from scams. Fraudulent emails can appear very convincing, using official language and logos, and even similar URLs. Always be alert.

Watch for attachments and typos

Your bank will never send attachments like a PDF in an unexpected email. Misspellings and poor grammar are also warning signs of a phishing scam.

What to do if you fall for an email scam

1. Change your password if you clicked on a link and entered any personal information like your username and password into a fake site.
2. Contact your bank by calling the number on the back of your card.
3. If you lost money, file a police report.
4. File a complaint with the Federal Trade Commission or call 1-877-FTC-HELP (382-4357).

American Bankers Association®

Phishing Red Flags

Every day, regular people like you lose their hard-earned money to online phishing scams. Don't fall for fake — learn how to spot shady texts, emails, and phone calls by knowing the things your bank would never ask.

BANKS NEVER ASK THAT .com

Phone Call Scams

Scammers sometimes try to cheat you out of your money by impersonating your bank over the phone. In some scams, they act friendly and helpful. In others, they'll threaten or scare you. Scammers will often ask for your personal information, or get you to send them money. Banks never will.

Watch out for a false sense of urgency

Scammers count on getting you to act before you think, usually by including a threat. Banks never will. A scammer might say "act now or your account will be closed," or even "we've detected suspicious activity on your account" — don't give into the pressure.

Never give sensitive information

Never share sensitive information like your bank password, PIN, or a one-time login code with someone who calls you unexpectedly — even if they say they're from your bank. Banks may need to verify personal information if you call them, but never the other way around.

Don't rely on caller ID

Scammers can make any number or name appear on your caller ID. Even if your phone shows it's your bank calling, it could be anyone. Always be wary of incoming calls.

Hang up—even if it sounds legit

Whether it's a scammer impersonating your bank or a real call, stay safe by ending unexpected calls and dialing the number on the back of your bank card instead.

What to do if you fall for a phone scam

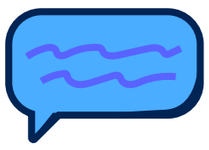
1. If you gave a scammer personal information like your SSN or bank account number, go to IdentityTheft.gov to see what steps to take, including how to monitor your credit.
2. Change your password if you shared any sort of username or password.
3. Contact your bank.
4. If you lost money, file a police report.
5. Report the scam to the Federal Trade Commission or call 1-877-FTC-HELP (382-4357).

American Bankers Association®

Phishing Red Flags

Every day, regular people like you lose their hard-earned money to online phishing scams. Don't fall for fake — learn how to spot shady texts, emails, and phone calls by knowing the things your bank would never ask.

BANKS NEVER ASK THAT .com



Text Message Scams

Phishing text messages attempt to trick you into sharing personal information like your password, PIN, or social security number to gain access to your bank account. As long as you don't respond to these messages and delete them instead, your information is safe. All you need to do is spot the signs of a scam before you click or reply.

EMAILS
PHONE CALLS
TEXT MESSAGES
MOBILE PAYMENT APPS

Slow down—think before you act

Acting too quickly when you receive phishing text messages can result in unintentionally giving scammers access to your bank account — and your money. Scammers want you to feel confused and rushed, which is always a red flag. Banks will never threaten you into responding, or use high-pressure tactics.

Don't click links

Never click on a link sent via text message — especially if it asks you to sign into your bank account. Scammers often use this technique to steal your username and password. When in doubt, visit your bank's website by typing the URL directly into your browser or login to your bank's mobile app.

Never send personal information

Your bank will never ask for your PIN, password, or one-time login code in a text message. If you receive a text message asking for personal information, it's a scam.

Delete the message

Don't risk accidentally replying to or saving a fraudulent text message on your phone. If you are reporting the message, take a screenshot to share, then delete it.

What to do if you fall for a phishing text message

1. Change your password If you clicked on a link and entered any sort of username and password into a fake site.
2. Contact your bank.
3. If you lost money, file a police report.
4. Report the scam to the Federal Trade Commission or call 1-877-FTC-HELP (382-4357).

American Bankers Association®

Phishing Red Flags

Every day, regular people like you lose their hard-earned money to online phishing scams. Don't fall for fake — learn how to spot shady texts, emails, and phone calls by knowing the things your bank would never ask.

BANKS NEVER ASK THAT .com

Mobile Payment App Scams

Scams using payment apps such as Cash App, PayPal, Venmo, or Zelle®, are growing more and more prevalent as those platforms become increasingly popular. Once you're hooked, it only takes seconds for a scammer to access your hard-earned cash.

Be wary of texts or calls about payment apps

Payment app scams often start with a phone call or text. If you get an unexpected call, just hang up. If you get an unexpected text, delete it. Even when they seem legitimate, you should always verify by calling your bank or payment app's customer service number.

Use payment apps to pay friends and family only

Don't send money to someone you don't know or have never met in person. These payment apps are just like handing cash to someone.

Raise the alarm on urgent payment requests

Scammers rely on creating a sense of urgency to get you to act without thinking. They might claim your account is in danger of being closed, or threaten you with legal action. These high-pressure tactics are red flags of a scam — a real bank would never use them.

Avoid unusual payment methods

Banks will never ask you to pay bills using a payment app, or ask you to send money to yourself. Scammers can "spoof" email addresses and phone numbers on caller ID to look like they're from your bank, even when they're not. When in doubt, reach out to your bank directly by calling the number on the back of your card.

What to do if you get scammed on a payment app

1. Notify the payment app platform and ask them to reverse the charge.
2. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.
3. File a police report.
4. File a complaint with the Federal Trade Commission or call 1-877-FTC-HELP (382-4357).

American Bankers Association®