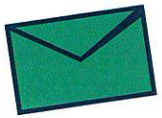
Phishing Scam Tips

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.

EMAILS

PHONE CALLS

TEXT MESSAGES

MOBILE PAYMENT APPS

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.

EMAILS
PHONE CALLS
TEXT MESSAGES
MOBILE PAYMENT APPS

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

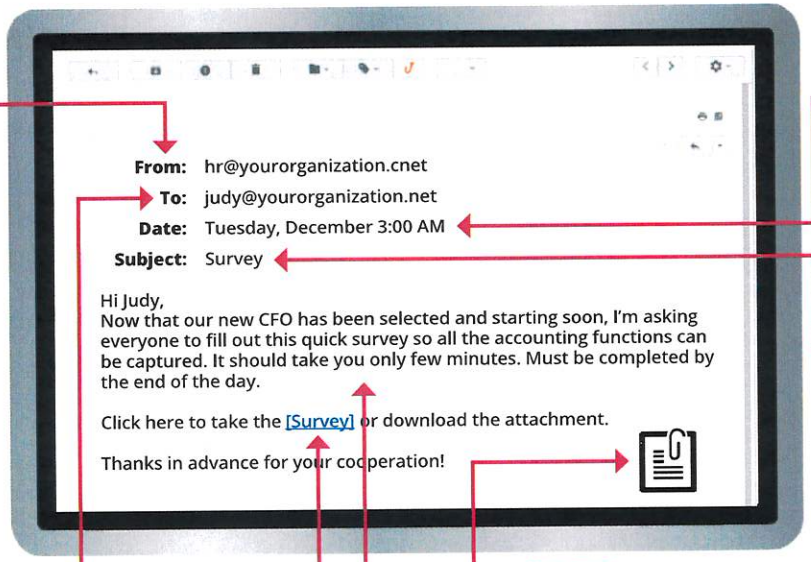
Banks will never ask you to pay bills using a payment app, or ask you to send money to yourself. Scammers can "spoof" email addresses and phone numbers on caller ID to look like they're from your bank, even when they're not. When in doubt, reach out to your bank directly by calling the number on the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

Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

Is someone using your personal or financial information to make purchases, get benefits, file taxes, or commit fraud? That's identity theft.

Visit IdentityTheft.gov to report identity theft and get a personal recovery plan.

The site provides detailed advice to help you fix problems caused by identity theft, along with the ability to:

- get a **personal recovery plan** that walks you through each step
- update your plan and track your progress
- print pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors

Go to **IdentityTheft.gov** and click "**Get Started**."

There's detailed advice for **tax**, **medical**, and **child identity theft** – plus over thirty other types of identity theft. No matter what type of identity theft you've experienced, the next page tells you what to do right away. You'll find these steps – and a whole lot more – at **IdentityTheft.gov**.

What To Do Right Away

Step 1: Call the companies where you know fraud occurred.

- ☐ Call the fraud department. Explain that someone stole your identity. Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.

- ☐ Change logins, passwords, and PINs for your accounts.

Step 2: Place a fraud alert and get your credit reports.

- ☐ To place a free fraud alert, contact one of the three credit bureaus. That company must tell the other two.
  - **Experian.com/help**
    888-EXPERIAN (888-397-3742)
  - **TransUnion.com/credit-help**
    888-909-8872
  - **Equifax.com/personal/credit-report-services**
    800-685-1111

  Get updates at **IdentityTheft.gov/creditbureaucontacts**.

- ☐ Get your free credit reports from Equifax, Experian, and TransUnion. Go to **annualcreditreport.com** or call 1-877-322-8228.

- ☐ Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

Step 3: Report identity theft to the FTC.

- ☐ Go to **IdentityTheft.gov**, and include as many details as possible.

Based on the information you enter, **IdentityTheft.gov** will create your Identity Theft Report and recovery plan.

Go to IdentityTheft.gov for next steps.

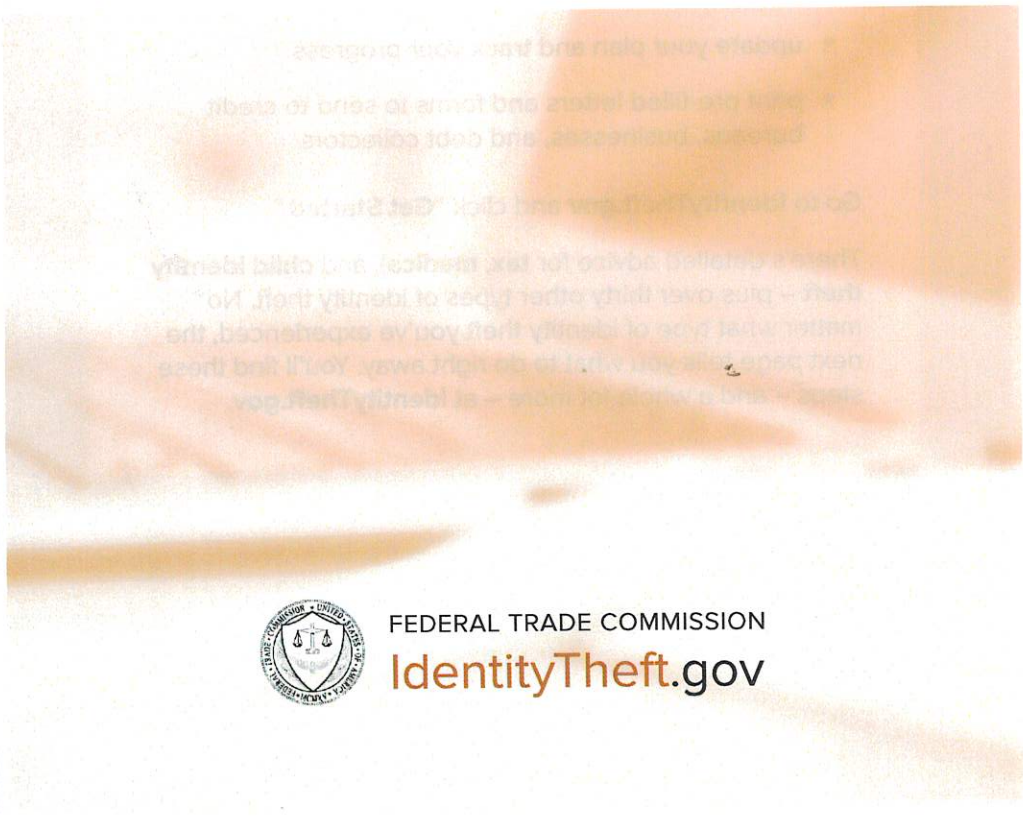
Your next step might be closing accounts opened in your name, or reporting fraudulent charges to your credit card company.

IdentityTheft.gov can help – no matter what your specific identity theft situation is.

FEDERAL TRADE COMMISSION
IdentityTheft.gov
September 2018

Identity Theft

What to know, What to do



FEDERAL TRADE COMMISSION
IdentityTheft.gov

Tips

1. Fraudsters are convincing and innovative in their techniques to trick you into giving up your assets, valuables, and information.
2. Always remember the federal government will never call you and ask for money.
3. Be vigilant about who you share your information with.
4. Make sure you verify their identities instead of disclosing yours.
5. Staying informed and aware is key to keeping your information, assets, and family members safe from financial fraud.

Learn more about financial scams at FBI.gov

Stop the fraud and report your complaint

If you believe you or someone you know may have been a victim of financial fraud, file a complaint with the FBI's Internet Crime Complaint Center (IC3)

IC3.gov or your local FBI field office

U.S. Department of Justice
Federal Bureau of Investigation
Financial Crimes Section
Economic Crimes Unit

Financial Fraud Awareness & Tips

Millions of people are victimized each year through financial schemes, generating losses in the hundreds of millions of dollars. Financial schemes target individuals of all ages and walks of life. Victims are lured with false promises of significant returns on investment, false claims about products and services, or the pretense that they can avoid fines or penalties.

Common Financial Schemes

- Investment fraud
- Romance or imposter scam
- Advanced fee scam
- Pandemic or disaster relief scam
- Elder fraud
- Identity theft

Investment fraud

Scammers induce investors to make purchases based on false or misleading information, typically by telling them an investment will yield a large return at little risk. An example is a Ponzi scheme, where new investments are used to pay fake "returns" to earlier investors.

Romance or imposter scam

Scammers trick a person into believing they're in a relationship (family, friend, romance, business, or government) and then persuade that person to send them money, personal or financial information, or other items of value.

Advanced fee scam

Scammers trick a person into paying upfront fees by promising larger gains later, which they never pay.

Pandemic or disaster relief scam

Scammers lure people into paying for illegal or fake pandemic- or disaster-related products or services.

Elder fraud

Scammers target people older than 60 through various scams.

Identity theft

Scammers either steal or coerce a person into giving up personally identifiable information, like a social security number or bank account information, and then use the information to commit fraud.

Do's

DO safeguard your personally identifiable information.

DO create strong passwords.

DO check your free credit reports.

DO verify a caller is legitimate by hanging up and calling a known provider number.

DO report fraud.

Don'ts

DON'T provide bank account information to unsolicited callers.

DON'T share passcodes.

DON'T provide remote access to your computer.

DON'T share personally identifiable information with anyone you don't know personally.