Scams & Fraud

Keep Your Money Safe
From Modern-day Thieves.

Fortifi Bank

What Is A Scam?

A scam is a deceptive scheme or trick used to cheat someone out of something valuable, typically money. Scammers use false promises, misleading information, or pretend to be someone they're not in order to steal from unsuspecting individuals.

SCAMS ARE ON THE RISE:
Per the Federal Trade Commission, in 2023, scammers stole over $10 billion from Americans — the highest ever recorded. From fake texts to online shopping scams, fraud is growing fast. Knowing the warning signs helps protect your money.

WHY SCAMS ARE COMMON NOW:
The digital surge during the pandemic has made scams more prevalent. Easy online transactions have helped scammers trick people into fraudulent activities quickly and effectively.

Common Scam Phrases

"ACT QUICKLY!"
Scammers use urgency to trick you.

"DON'T TELL YOUR BANKER."
A sure sign of a scam.

"DON'T TRUST OTHERS."
Scammers isolate you from help.

"DO THIS OR FACE ARREST."
False threats are scam tactics.

"STAY ON THE LINE."
They're stalling to scam you.

"USE A BITCOIN ATM."
Real requests don't involve crypto ATMs.

When in doubt, hang up and consult with someone you trust.

Tips To Stay Safe

USE STRONG PASSWORDS: Never share a password or write it down. Strong passwords are multiple characters, usually including an upper case, special character and number.

VERIFY THE SOURCE: Avoid communicating with someone you do not know. Instead, stop the conversation and reconnect back directly with the person that you know.

DO NOT SHARE PERSONAL INFORMATION: A bank or creditor will never call you asking you to share your account number or SSN.

DON'T CLICK LINKS: If you do not know the sender, do not click a link or open a file.

STAY CALM: Scammer's like to get people to take action quickly. Legitimate businesses will give you time to make a decision.

Is It Fraud? TAKE THE QUIZ

IS THIS A STRANGER? Did the contact come from an unverified person or entity asking for personal information? Did you meet this person on Facebook or other social media?

IS IT URGENT? Are you being pressured to act immediately without time to think or consult?

ARE YOU EMOTIONAL? Does the situation play heavily on your emotions, like sympathy or fear?

DO YOU NEED TO PAY IN A SPECIFIC WAY? For example, you must use a gift card or bitcoin.

IS IT OVERSEAS? Does the transaction involve sending money overseas or electronically, such as through wires, bitcoin, or gift cards?

If you answered "YES" to any of the questions above, you could be involved in fraud.

Common Scams

Scammers are constantly finding new ways to trick people. Community banks, like Fortifi Bank, regularly see these types of scams affecting local individuals and businesses. Stay informed about these common scams to recognize warning signs and protect yourself and your money.

IMPERSONATION SCAMS

Grandparents Scam

Scammers impersonate a grandchild in distress, playing on grandparents' emotions to trick them into sending money urgently.

Romance Scam

Scammers create fake online personas, develop relationships, and then deceive victims into sending money for emergencies.

Charity Scam

Scammers exploit your generosity by posing as fake charities to steal donations, especially after natural disasters or during holidays.

Vishing Scam

Scammers phone you, pretending to be officials or service providers, to coerce you into sharing personal and financial information.

TECHNOLOGY SCAMS

Tech Support Scam

Scammers claim your computer has a virus and offer to fix it, gaining remote access to your system to steal sensitive information.

Crypto Scam

Promises of high returns on crypto-currency investments lead to fraudulent schemes where your investment is stolen by scammers.

Phishing Scam

Fraudsters send emails mimicking legitimate companies to trick you into giving away personal details like passwords and bank info.

Text Message Scam

Unsolicited texts with links lead to fake websites designed to steal your personal information or install malware on your device.

Online Shopping Scam

These involve fake retail sites or false ads on legitimate sites to lure shoppers into buying products that will never be delivered.

Robocall Scam

Pre-recorded calls make false claims of prizes or legal threats, trying to extract your personal data or payments.

FINANCIAL SCAMS

Fake Banker Scam

Scammers pose as bank employees to 'verify' your account details due to 'suspicious activity,' aiming to access your funds.

Unsafe Account Scam

Con artists alert you to a 'breach' and advise you to 'confirm' your banking details, leading to potential account compromise.

Credit Card Scam

These scams might involve offers for credit cards with exceptional benefits. Scammers seek upfront payment or personal information.

Fake Lottery Scam

You're told you've won a big prize and must pay a fee to claim it. There's no prize, and the fee goes straight to the scammers.

False Investment Scam

Offers of no-risk, high-return investments that, in reality, funnel your money into the pockets of fraudsters.

Debt Collection Scam

Scammers pose as debt collectors and trick people into paying debts they don't owe or have already paid.

Common Scam Methods

Scammers tend to reach out via a few common methods. Always verify unexpected contacts carefully.

PHONE:
Impersonating officials or services.

EMAIL:
Impersonating trusted entities.

TEXTS:
Sending alerts or offers.

POP-UPS:
Fake warnings or deals online.

SOCIAL MEDIA:
Posing as contacts or brands.

WEBSITES:
Fake sites asking for info.

MAIL:
Soliciting through posted letters and may include a fake QR code.

Already Gave Information?

If your personal information has fallen into the wrong hands, quick action can limit the damage. Follow these immediate steps to protect your financial security:

DID YOU GIVE BANK CARD INFORMATION?

1. Turn your card off immediately using Fortifi's online or mobile banking, and call Fortifi right away to cancel and replace the card. (855.876.1500)
2. Update any automatic payments linked to the canceled card.

DID YOU GIVE ACCOUNT CREDENTIALS?

1. Reset any details to the account including username and passwords.
2. Apply these changes across all accounts if your PC was accessed.

DID YOU GIVE COMPUTER ACCESS?

1. Reset all of your email login usernames and passwords.
2. Get your computer checked by a trusted technician to rule out malware.

Trust Your Banker

At Fortifi Bank, safeguarding your finances is a tradition we've upheld for 150 years, right here in Wisconsin. Your banker is trained to help identify fraud and guide you through secure banking practices.

How does Fortifi Help?

Fortifi Bank teaches you about avoiding scams and question if something seems off. We can keep you safe with optional tools like ACH block and filter, postive pay, two-factor authentification, debit card on/off, and the ability to recieve alerts on your phone.

ARE YOU A VICTIM?

If you believe you have been involved in a scam or fraud, call 855.876.1500 immediately.

Scan to learn more

FortifiBank.com/Fraud

Updated 3.2025