



TO PROTECT YOURSELF AND SAFEGUARD YOUR FINANCIAL WELL-BEING, FAMILIARIZE YOURSELF WITH COMMON TYPES OF SCAMS SO YOU CAN SPOT THEM, NOT FALL FOR THEM!

Scammers use a variety of tactics to persuade their victims into falling for their schemes, including acting friendly, helpful, and sympathetic, or using fear tactics. Their communications will most likely be from a phone number, email, or person you've never seen before. These fraudsters often create a fake sense of urgency to cause panic or confusion, and may ask for payment in a complicated method. A good rule of thumb is: if it's too good to be true... it probably is!

Should you become the victim of a scam, it is incredibly difficult to recover money that you willingly sent. If you suspect you're being or have been scammed – stop communication with the fraudster immediately and call your financial institution connected to your method of payment.

Common Scams Include:

Business Email Compromise Scams

You receive an email from your supplier/vendor requesting to send money to a different account. The supplier/vendor email appears to be familiar. But this could be a fraudster who obtained access to the network of your supplier/vendor.

Charity Scams

You receive a request to donate to a charity that you've never heard of and for which you can't find an official website.

Check Cashing

You're approached outside a bank branch and asked to cash a check for someone who claims they don't have an account or left their ID home. The bad check will be held against your account when it doesn't clear.

Compromised Card Scam

Scammers call claiming to be from your bank and say that your card has been compromised. They'll attempt to send someone to your home to "secure" your account by destroying your card. Though they may seem to be legitimate, once they have possession of the card, they'll use it to steal money from the account.

Debt Relief

You receive a request for payment in order to establish a service relationship to pay, settle or get rid of debt.

Employment Scams

Be vigilant in validating employment opportunities, especially when exclusively online or working from home. Be suspicious if someone claims to have overpaid you for a job, promises to reimburse for equipment, or asks you to send equipment to an IT dept. The equipment may never be returned, and reimbursements or overpayments may be illegitimate, leaving you liable for the funds. Never divulge personal information online to an unreliable source or through deceptive job

Fake Rental

A house is legitimately listed for sale online, but scammers have set up a fake website and listed the house as a rental. You send your first month's deposit to a scammer pretending to be the landlord/owner.

Fake Websites

Legitimate-looking websites are being created by scammers, and a quick Google search will lead you to a real-looking phone number. When you call, they'll try to obtain your sign-in details or other information.

FTC / IRS Scams

Scam artists are pretending to be IRS officials to get your money. They'll call, email, or text you claiming you owe back taxes or there's a problem with your tax return. They even rig caller ID to make their call look official. They play on your fears.

Grandparent Scam

You receive a call or text message from someone claiming to be a grandchild or loved one asking for money to help with an emergency, plus instructions on where to send the funds.

Impersonation Scams

Scammers pose as a legitimate company or a utility company and request personal information or a payment transfer in order to make things "right" on your account. They might also use a fake caller ID that could show up as a legit company's number and/ or request remote access to your device. Scammer posing as a utility company might warn you to pay your balance within a limited time or else the utility will be shut off.

Investment Scams

You receive a request to invest in a business opportunity with promises of high returns and/or getting rich quickly.

Lottery Scams

You receive a request to prepay fees or taxes in order to receive a large prize you supposedly won.

Mortgage Closing

You receive an email or text message that looks similar to your real estate agent's contact info that indicates there is a last minute change to the wiring instructions, and tells you to wire closing costs to a different account.

Online Merchant/Marketplace Scams

When responding to ads or interacting in marketplaces on social media, research sellers and products independently to ensure legitimacy. Notice the red flags like a high-ticket item for a price too-good-to-be-true or a buyer who "accidentally" overpaid you for an item or someone asking for personal information or redirecting to an unfamiliar/strange looking URL.

Overpayment Scams

You receive an overpayment for an item you're selling, immediately followed by a request to deposit the check (which turns out to be a bad check) and then send the difference via a wire or gift card.

Payment Scams

Be wary if you are urged to make a purchase with the promise of compensation, or if someone offers to make a payment for you, or provides you with bank account info with which to make a payment. If you use a payment method you are not familiar with, you run the risk of ultimately being held responsible for the amount paid.

Puppy Scam

Scammers post fake litters online or pretend to be someone they're not (usually an existing breeder) to take advantage of puppy sales (sans the puppies.)

QR Code Scams

When scanning QR codes, use your smartphone's default camera app to avoid scams and potential fraud. Scammers use 3rd party QR code scanner apps and/or the ads within the apps to direct users to fake or malicious websites designed to obtain your personal information.

Romance Scams

If you are asked for financial support from a new partner in a relationship that's been exclusively online, you're likely a target of this elaborate scheme.

Tech Support Scams

Tech support claims your computer has malware and requests payment to fix the defects or access your computer.