Common Types of Fraud & Scams

Fraudsters are getting smarter every day and continually inventing new methods to get your information and money.

All schemes are designed to get one of two things: your money or the passwords and other data that can be used to get your money. The moment you receive a request, it's time to slow down, get suspicious, and verify the claim or offer.

Mobile Banking Scams

Fraudsters contact their victims through email or social media posing as a potential employer or lender. The fraudster will oftentimes provide the victim with an opportunity to earn quick money by depositing a check to your account or by asking for help in moving money from overseas. The fraudster will further request your bank account information and may even ask for your online or mobile banking login and password. The fraudster uses the information to deposit a fake check. Once the deposit has been made, the scammer will request funds to be immediately transferred back to them via money order, person to person transfer, wire transfer, reloadable cards or even gift cards, i.e., Google Cards. After funds have been sent to the scammer, the check or checks that were deposited will be returned and the funds will be removed from the victim's account, causing a loss to the victim.

Avoid falling prey to these scams by following these few simple steps:

- Never give out personal information to strangers. This includes your debit card number, PIN, bank account number, and any online or mobile banking login information or information regarding gift cards purchased.
- If you are offered money in exchange for your personal information, it's likely a scam. Don't proceed. Scammers could leave you owing thousands.
- Check your online bank statements regularly. If you see something unfamiliar, call your bank or credit union immediately.
- If you apply for a work-from-home job by email or online and the first thing they do is send you a check to cash then request you to return some or all of the money to them, it's most likely a scam.

Tax Scam

Criminals take advantage of every opportunity to prey on unsuspecting individuals, and tax filing season is no exception. Scammers use the regular mail, telephone, or email to set up individuals, businesses, payroll and tax professionals.

IRS impersonation scams, thieves make unsolicited phone calls to their intended victims fraudulently claiming to be from the IRS. In this most recent scam variation, callers' "spoof" the telephone number of the IRS Taxpayer Advocate Service office in Houston or Brooklyn. Calls may be 'robo-calls' that request a call back. Once the taxpayer returns the call, the con artist requests personal information, including Social Security number or individual taxpayer identification number (ITIN).

In other variations of the IRS impersonation phone scam, fraudsters demand immediate payment of taxes by a prepaid debit card or wire transfer. The callers are often hostile and abusive.

Alternately, scammers may tell would-be victims that they are entitled to a large refund but must first provide personal information. Other characteristics of these scams include:

- Scammers use fake names and IRS badge numbers to identify themselves.
- Scammers may know the last four digits of the taxpayer's Social Security number.
- Scammers spoof caller ID to make the phone number appear as if the IRS or another local law enforcement agency is calling.
- Scammers may send bogus IRS emails to victims to support their bogus calls.
- Victims hear background noise of other calls to mimic a call site.

After threatening victims with jail time or with, driver's license or other professional license revocation, scammers hang up. Others soon call back pretending to be from local law enforcement agencies or the Department of Motor Vehicles, and caller ID again supports their claim.

Tax refund identity theft happens when bad actors get their hands on your personal information, such as your name, date of birth and/or Social Security number that they then use to file a fraudulent tax return and obtain a refund. One of the easiest ways to help prevent this is to file your tax return early – before an identity thief has the chance to file a fake one.

If you're a taxpayer and you notice a refund you weren't expecting in your bank account, this is a clue you might be victim of tax fraud. This will typically be followed by a call to let you know that it was deposited accidentally and to transfer to an account posing as the IRS. The first step is to notify us. You will probably need to close the account since the bad guys now have your bank account information. The second thing to do is to contact the IRS to let them know you suspect you're a victim of fraud. Finally, if you haven't been in contact with your tax preparer, you should contact his or her office to let them know their data might have been compromised.

The IRS will never:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- Threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone.
- Call about an unexpected refund.

Count Confirmation/Service Scams

Telephone call, email message, or text message from what seems to be a legitimate company asking for the recipient to provide their personal or account information to address an issue concerning their account ("we suspect an unauthorized transaction", "your debit card has been deactivated, to reactivate…", "we are conducting our regular account verification process", etc.). The recipient is asked to provide the information directly over the phone, or in the case of email and text, directed to a fraudulent website or customer service number.

Check Cashing Scams

A request from a fraudster for the recipient to deposit a check for the sender and wire them the proceeds. In exchange for their effort, the recipient is told to keep a portion of the check. Inevitably, the check will be returned as counterfeit and the recipient will be liable for the full amount of the check.

Sweetheart Scams

Also known as a romance scam, this is a scam most notably used on online dating sites on which a fraudster develops a romantic relationship with their victim. Eventually, the fraudster requests money or personal information.

Work-at-Home Scams

In this scenario the victim will respond to a work-at-home employment offer. Most of the offers will take the form of an invoice or payroll processing position that only requires an active bank account. The fraudster will move funds into the victim's account with instructions to wire portions of those funds to pay "vendors". An alternate version has the fraudster requesting that the victim wire funds to cover onboarding and training costs for the new position.

Tech Support Scams

Someone will present themselves to the victim as technical support for a well-known software or hardware vendor and will convince the victim to provide access to their computer, to unknowingly install malicious software or to provide credit card information for payment. A variation of this scam involves the victim receiving a pop-up message alerting the victim to a virus and asking them to install free security scanning software to remove the virus, again resulting in the victim installing malicious software on their computer.

Please visit the Consumer Financial Protection Bureau (CFPB) Link for other published scams and learning how to protect yourself and other from fraud and scams.

https://www.consumerfinance.gov/consumer-tools/fraud/