10 Most Common Frauds According to the FDIC

Scam artists have become increasingly sophisticated over the years, but remembering a few simple rules can be surprisingly effective at keeping your money safe.

One of the stalwarts is to avoid offers that seem too good to be true, especially if you're being pressured to act fast or to keep a transaction secret, said Michael Benardo, manager of the cyber fraud and financial crimes section at the Federal Deposit Insurance Corp. (FDIC) which often hears from bank customers who've been victimized.

In addition, be cautious of unsolicited emails or text messages that ask you to open an attachment or click on a link. That's a common way for cybercriminals to infect your computer with malicious software, which can steal your personal financial information or spy on you by capturing your keystrokes, Benardo said.

And no matter how legitimate an offer or request may sound, don't give out sensitive personal data such as bank account, Social Security or credit card numbers or passwords to anyone unless you initiate the contact and know the party is reputable, he said.

In an effort to educate consumers about what to watch out for, the FDIC recently released a list of 10 common frauds targeting bank customers.

Government "impostor" frauds. These schemes start with a phone call, letter, email or text message supposedly from a government official demanding an upfront payment or personal financial information. In the IRS scam, for example, the crook claims you owe back taxes that must be paid immediately. "They might even threaten you with a lawsuit or arrest if you don't pay," Benardo said. Federal government agencies won't ask people to send money for prizes or unpaid loans, and won't ask for money to be wired, he said. Another common impostor scam involves thieves pretending to be from Microsoft or a technology repair service and claiming the person's computer was infected with a virus. They then trick people into installing malicious software used to steal personal data, and may demand payment to remove the software.

Debt collection scams. Fraudsters pose as debt collectors or law enforcement officials attempting to collect bogus debts. Red flags include a caller who won't provide written proof of the debt, or threatens arrest or violence for not paying.

Fraudulent job offers. These ploys often involve work-at-home offers in which prospects are required to pay money in advance or provide personal financial information. One variation involves fake part-time jobs as a "mystery shopper" visiting stores and submitting reports about the experience. Or the job might be to receive a $500 check, go "undercover" to a bank, deposit the check into an account, and report back on the service after wiring the "employer" $500 to cover the check, which turns out to be counterfeit.

Phishing emails. These involve legitimate-looking emails purporting to be from a bank or other popular entity asking for personal information. They may direct people to fake websites that appear to be exact copies of real websites, except for a slightly different web address.

Mortgage foreclosure rescue scams. These entail promises to refinance a mortgage under much better terms. They may include significant upfront fees, or trick the homeowner into signing documents that transfer ownership of the property to the criminal. Common warning signs include a "guarantee" that foreclosure will be avoided and pressure to act fast.

Lottery and sweepstakes scams. Potential victims are told they've won a big prize, but must first send in money to cover taxes and other fees.

Elder frauds. Senior citizens are a major target of crooks trying to cheat them out of their life savings. Warning signs include unsolicited phone calls asking for a large amount of money before receiving goods or services, and special offers for seniors that seem incredible, such as an investment guaranteeing a high return.

Overpayment scams. These typically involve a thief sending a check for something someone is selling, but for more than the asking price. The scammer tells the seller to deposit the check and wire the difference back. In a few days, the check bounces, and the victim is out the money, plus the merchandise that already may have been sent.

Ransomware. This malicious software holds a computer or smartphone hostage by restricting access until the victim pays a ransom. Ransomware is commonly spread when someone clicks on an infected email attachment or link leading to a contaminated site. The malware can be passed around on a contaminated storage device, such as a thumb drive.

Jury duty scams. A thief calls pretending to be a law enforcement official warning that the person failed to appear for jury duty and will be arrested unless a "fine" is paid immediately. The caller may ask for debit account and personal identification numbers, which are then used to create a fake debit card and drain the victim's account.

What You Can Do: The basics on how to protect your personal information and your money

Here are some basic precautions to consider, especially when engaging in financial transactions with strangers through email, over the phone or on the internet.

- Avoid offers that seem "**too good to be true**." "If someone promises 'opportunities' that are free or with surprisingly low costs or high returns, it is probably a scam. Be especially suspicious if someone pressures you into making a quick decision or to keep a transaction a secret."
- No matter how legitimate an offer or request may look or sound, **don't give your personal information**, such as bank account information, credit and debit card numbers, Social Security numbers and passwords, to anyone unless you initiate the contact and know the other party is reputable.
- Remember that financial institutions will not send you an email or call to ask you to put account numbers, passwords or other sensitive information in your response because they already have this information. To verify the authenticity of an email, independently contact the supposed source by using an email address or telephone number that you know is valid.
- Be **cautious of unsolicited emails or text messages** asking you to open an attachment or click on a link. This is a common way for cybercriminals to distribute malicious software, such as ransomware. Be especially cautious of emails that have typos or other obvious mistakes.
- Use **reputable anti-virus software** that periodically runs on your computer to search for and remove malicious software. Be careful if anyone (even a friend) gives you a thumb drive because it could have undetected malware, such as ransomware, on it. If you still want to use a thumb drive from someone else, use the anti-virus software on your computer to scan the files before opening them.
- **Don't cash or deposit any checks, cashier's checks or money orders from strangers** who ask you to wire any of that money back to them or an associate. If the check or money order proves to be a fake, the money you wired out of your account will be difficult to recover.
- Be wary of **unsolicited offers "guaranteeing**" to rescue your home from foreclosure. If you need assistance, contact your loan servicer (the company that collects the monthly payment for your mortgage) to find out if you may qualify for any programs to prevent foreclosure or to modify your loan without having to pay a fee. Also consider consulting with a trained professional at a reputable counseling agency that provides free or low-cost help. Go to the U.S. Department of Housing and Urban Development website for a referral to a nearby housing counseling agency approved by HUD or call 1-800-569-4287.
- **Monitor credit card bills** and bank statements for unauthorized purchases, withdrawals or anything else suspicious, and report them to your bank right away.
- Periodically **review your credit reports** for signs of identity theft, such as someone obtaining a credit card or a loan in your name. By law, you are entitled to receive at least one free credit report every 12 months from each of the nation's three main credit bureaus (Equifax, Experian and TransUnion). Start at AnnualCreditReport.com or call 1-877-322-8228. If you spot a potential problem, call the fraud department at the credit bureau that produced that credit report. If the account turns out to be fraudulent, ask for a "fraud alert" to be placed in your file at all three of the major credit bureaus. The alert tells lenders and other users of credit reports that you have been a victim of fraud and that they should verify any new accounts or changes to accounts in your name.
- **Contact the FDIC's Consumer Response Center** (CRC) if you have questions about possible scams or you are the victim of a scam experiencing difficulty resolving the issue with a financial institution. The CRC answers inquiries about consumer protection laws and regulations and conducts thorough investigations of complaints about FDIC-supervised institutions. If the situation involves a financial institution for which the FDIC is not the primary federal regulator, CRC staff will refer the matter to the appropriate regulator. Visit our webpage on submitting complaints or call 1-877-ASK-FDIC (1-877-275-3342) Monday - Friday, 8am to 8pm (EST).