Ten Scams Targeting Bank Customers

The basics on how to protect your personal information and your money

The FDIC often hears from bank customers who believe they may be the victims of financial fraud or theft, and our staff members provide information on where and how to report suspicious activity. As part of that coverage, we feature here a list of scams that you should be aware of, plus key defenses to remember.

Government "imposter" frauds. These schemes often start with a phone call, a letter, an Email, or a fax supposedly from a government agency, requiring an up front payment or personal financial information, such as Social Security or bank account numbers.

Debt collection scams. Be on the lookout for fraudsters posing as law enforcement officials attempting to collect a debt that you don't owe. Red flags include a caller who won't provide written proof of the debt you supposedly owe or who threatens you with arrest.

Fraudulent job offers. Criminals pose online or in classified ads as employers or recruiters offering opportunities, such as working from home. But if you're required to pay money in advance to "help secure the job" that's a red flag of a potential fraud.

Phishing Emails. Scam artists send Emails pretending to be from banks, and they ask for personal information. The Emails usually look legitimate because they include graphics copied from authentic Websites and messages that appear valid.

Mortgage foreclosure rescue scams. Borrowers should always be on the lookout for scammers who falsely present homeowners with the life-saving offer they need. Instead, the homeowner is required to pay significant up front fees or, even worse. Common warning signs of a "guarantee" that foreclosure will be avoided.

Lottery scams. You might be told you won a lottery and asked to first send money to the "lottery company" to cover certain taxes and fees.

Elder frauds. Thieves sometimes target older adults to try to cheat them out of some of their life savings. For example, telemarketing scams may involve sales of bogus products and services that will never be delivered.

Jury duty scams. A thief makes phone calls pretending to warn innocent people that they failed to appear for jury duty and threatening an arrest unless a "fine" is paid. And to pay up, the caller asks for debit account and PIN numbers, allowing the perpetrator to create a fake debit card and drain the account.

What You Can Do

While we have described many forms of financial scams, the red flags to look out for are often similar. And so are the things you can do to help protect yourself 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."
- 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, 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.
- 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.
- Use reputable anti-virus software that periodically runs on your computer to search for and remove malicious software.
- 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.
- 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.

Contact the FDIC's Consumer Response Center (CRC) if you have questions about possible scams. Call 1-877-275-3342.

Article and Images from Federal Deposit Insurance Corporation

SCAMS & SAFETY

Fraud Against Seniors

The FBI's Common Fraud Schemes Webpage provides tips on how you can protect yourself and your family from fraud. Senior citizens especially should be aware of fraud schemes for the following reasons: Senior citizens are most likely to have a "nest egg," to own their home, and/or to have excellent credit—all of which make them attractive to con artists.

People who grew up in the 1930s, 1940s, and 1950s were generally raised to be polite and trusting. Con artists exploit these traits, knowing that it is difficult or impossible for these individuals to say "no" or just hang up the telephone.

Older Americans are less likely to report a fraud because they don't know who to report it to, are too ashamed at having been scammed, or don't know they have been scammed. Elderly victims may not report crimes, for example, because they are concerned that relatives may think the victims no longer have the mental capacity to take care of their own financial affairs.

Senior citizens are more interested in and susceptible to products promising increased cognitive function, virility, physical conditioning, anti-cancer properties, and so on. In a country where new cures and vaccinations for old diseases have given every American hope for a long and fruitful life, it is not so unbelievable that the con artists' products can do what they claim.