How to avoid these 12 scary money scams

By Paul Sisolak GoBankingRates.com September 21, 2015 - 9:53pm

Scammers have been around since the beginning of time. As long as there have been vulnerable people with money, there has been someone looking to steal it.

Today, the classic bait-and-switch comes in many new and sophisticated varieties updated for the 21st century. There is a new breed of high-tech scam just waiting to dupe you out of your money.

To avoid becoming another unwitting victim and putting your finances at risk, keep an eye out for these 10 increasingly common money scams.

1. The 'Flipping Money' Scam

The scam: You might have heard of flipping a house, where you buy a cheap house, renovate it and sell it at a higher price for profit. Flipping is not a scam when it is done properly and legally. But a new get-rich-quick scheme popping up on social media is a bona fide hustle.

In this money-flipping scam, Facebook, Twitter and Instagram users are lured to ads with promises to turn $100 into $1,000. According to AZCentral.com, victims are asked to put money on a pre-paid debit card and contact the scammers via phone or text message. They are then asked to provide the scammers with the card's personal identification number. The scammers use this information to retrieve the money and are never heard from again.

The solution: Do not fall for empty promises to multiply your money, and never hand your funds over to strangers.

2. Ransomware

The scam: Perhaps you are innocently surfing the internet when you click on the wrong page. Or, you get an email in your inbox that claims it is from a familiar friend with an attachment that you open. Suddenly an oversized FBI logo appears on your screen, along with a message claiming that your IP address was involved in illegal downloading of pornographic materials. Your computer freezes up, and you won't be able to close the window or divert away unless you pay up.

Known as "ransomware," this is a derivative of spyware and malware. According to NJ.com, ransomware scams often demand you hand over cash via payment services such as Bitcoin or MoneyPak.

The solution: Be careful of the places you visit on the Web and the links you click. To prevent stumbling onto the wrong site, keep your antivirus software always updated with the latest patches. If your computer is infected, have a computer technician remove the offending virus. Another remedy is to shut down your computer, restart in safe mode and download software such as RogueKiller to do the work. Then, go into your browser history and delete the offending ransomware link.

3. Phishing and Vishing

The scam: With phishing, fraudsters impersonate a business or official agency — such as the police or your bank — and get you to click on a link in a text or email that directs you to a website asking you to divulge your personal information, Social Security number or checking account number. "Vishing" is the phone version of phishing; here, a scammer will call up a victim claiming to be either a bank representative or the authorities.

The caller might suggest that your account has been hacked or compromised. Then, he or she will offer to solve the problem over the phone if you hand over your security information. According to ID theft expert Robert Siciliano, one version of this

scam fools victims into paying unpaid taxes. In such a case, the fraudster might even use spoof technology so an official phone number appears on your caller ID.

The solution: To protect yourself, be on the lookout for red flags. "Phishers are not known for their grammar and spelling," said Haroon Ahmad, director of public relations for JotForm, the first Web-based WYSIWYG form builder. "If you notice mistakes in an email or a form, it might be a scam."

He added that consumers should look for phony email links. "Most phishers try to send you to a fake site with a form for you to fill out," he said. "Hover your mouse over the link to see if the address matches the link that was typed in the message."

Never divulge sensitive information over the phone. If you receive a call from someone purporting to be the police, hang up the phone, call the real police and report the incident. Your bank will never resolve hacking or fraud crimes strictly over the phone.

4. Phony and Copycat Mobile Apps and Websites

The scam: Mobile apps have become the standard vehicle for handling a lot of banking and financial business. Scammers have latched onto that fact as a way to make money off your money. Many victims of this type of fraud are tricked into downloading a fake payment app that looks legitimate. Instead, this phony app contains a malicious virus that allows thieves to steal money directly from your bank account. Just when you think your peer-to-peer payment or account transfer went through, the funds actually have landed in the hands of some anonymous thief.

The solution: Experts suggest only downloading from and doing business with reputable websites and mobile apps, such as Mint, Venmo and Square Cash. Do not download new apps unless they come from reputable sources such as iTunes or Google Play.

Get to know your Web browser abbreviations to verify if a site is legit. According to debt relief expert Harrine Freeman, the URL or website address should start with "http://," "https://" or "shttps://." "Cut and paste the URL in the Google search box; if no results are returned, the website is not legitimate," Freeman said.

5. The 'Missed Jury Duty' Telemarketing Scam

The scam: One day, your phone rings. The caller purports to be the clerk of your local court, claiming you missed jury duty and that you will be arrested immediately unless you pay a substantial fine. Just like phishing, this impostor scam works under the guise of intimidation. "The court jury system does not work this way," said Lynn Edgington, author and cyber-crime expert. "They scare you into thinking you are going to jail and, of course, they provide you with the instructions as to where you are to wire the money."

The solution: Don't believe a word of anyone who makes a call of this nature. If you truly miss jury duty, you will be notified by mail that you are in contempt of court. Matters of this sort are not handled over the phone but in front of a judge.

6. Apartment Rental Scams

The scam: Apartment hunters — especially first-timers looking for their own place — can be especially vulnerable to a host of scam listings on Craigslist and other sites. MarketWatch warns consumers to be wary of online apartment listings that look real but have been manipulated. "Scammers will hijack a rental listing, swap out the contact information for their own and place it on another site," she wrote. "In some cases, they don't even change the contact info, they hack the landlord or property manager's email address."

Then there are phony/phantom listings for apartments that don't exist. The "landlord" contacts prospective tenants, asking them to wire a security deposit or first month's rent.

The solution: Suspect fraud if the person requesting something from you will not arrange to meet you. "If the owners or managers ask for a security deposit or first month's rent before you've met or signed a lease, it may be a scam," according to MarketWatch. "If you can't be there in person to see the apartment, ask someone you trust to go in your place. This will ensure

that apartment is indeed for rent as advertised." You also should conduct an internet search on the owner, according to MarketWatch, because an ad listed under different names can be a clear sign of a scam.

7. Senior Citizen Scams

The scam: Senior citizens are particularly susceptible to being targeted by scammers. Many seniors fall prey to cold callers and texters offering advice on pension, retirement and investment help. There aren't too many depths that fraudsters aren't willing to sink to; many scammers will impersonate charities, funeral homes, nonprofits and even family friends with a sob story, according to Siciliano's blog.

Such scams typically end with trusting seniors giving away personal or bank account information. Some scammers even show up at seniors' doorsteps. In what is known as a "medical alert" scam, retirees receive a call or visit from a representative of a mysterious company who claims that a family member or friend ordered a medical device for the retiree. According to Global News, the scammer will demand payment and walk off with the senior's a debit or credit card number, checking account routing sequence, or cash.

The solution: Seniors need to stay alert. Don't ever divulge sensitive information to anyone over the phone, on the internet or in an email. If you're not savvy about computers or the internet, take a basic skills course to better understand how these technologies work and how to protect yourself from cybercrime. If you have an elderly parent or grandparent, talk to them about staying safe over the phone or online.

8. 'Cracking Card' Scams

The scam: Younger generations aren't immune to today's newer money scams. Aimed mostly at millennials and college students in need of money, the "cracking card" scam involves asking victims to hand over their personal identification number or debit card information to get a percentage of the scammer's "bank deposit," which is actually made up of counterfeit checks that were created by the con artist.

According to USA Today, participants are promised anywhere from 10 percent to half of the deposit. While some of the recruited participants are fully aware of their participation in such an illegal scheme, others are not, USA Today reported.

The solution: USA Today noted that the "cracking cards" scheme has reportedly cost banks across the nation about $11.6 million in stolen consumer money. To avoid being victimized by this type of scam, be wary of any offer that promises to put cash in your hands quick. Don't ever leave your personal identification number in view for strangers and scammers to see. According to the USA Today report, "Authorities also have warned college students to be careful about providing any banking account information in relation to a job prospect, maybe under the guise of running a credit check."

9. The Fake Tech Support Scam

The scam: Not unlike a phishing scheme, victims of this scam are duped by phony computer tech support reps into paying money for repairs that are not needed. "We have had several customers report that they receive a phone call from someone who claims to be from Microsoft," said Raymond Delien, owner of The Desk Doctors, a computer repair and IT consulting business. "They tell them that their computer is reporting serious errors to Microsoft."

According to Delien, the fake repair people direct victims to click on their computer's event viewer, where the "errors" are taking place. "They then tell you they can fix it for $300, and they have you connect them and then they start to fiddle and fidget," Delien adds. "They can download malware, and when they are done, they charge your credit card for as much as they want."

Another version is the "WiFi scam": "You connect to free WiFi thinking you're secure, but waiting in the wings is a hacker to sniff out your data," Siciliano wrote on his blog.

The solution: Computer companies aren't monitoring your activity and would have no clue if you are experiencing technical difficulty. Simply hang up if you are on the receiving end of one of these calls and invest money in some good antivirus

software. As far as protecting your ID over an open network, several experts recommend that computer users opt for a virtual private network, or VPN, anytime they log on to the internet.

10. Tax Refund Fraud

The scam: When scammers get hold of your Social Security number and tax filing information, they can wreak havoc on your finances. It's a sneaky, yet straightforward, form of identity theft. According to Howard Gleckman of Forbes, "Crooks steal Social Security numbers, file returns that claim refunds, and have the refunds electronically deposited into fake bank accounts or delivered to mail drops. Not only do they steal money from the government, but they create an enormous headache for legitimate taxpayers whose IDs they have stolen."

The solution: Be proactive with your finances and taxes. If you believe you've been the victim of tax fraud, contact the authorities and the IRS. It goes without saying that you shouldn't give out your tax or Social Security information to anyone you don't trust.

11. Ponzi Schemes

The scam: Who can forget the Ponzi scheme Bernie Madoff pulled off for more than three decades? Named after 1920s scammer Charles Ponzi, a Ponzi scheme promises investors unbelievably high returns. In reality, hardly any money is being invested — instead, investors like Madoff essentially pocket the money for their own gain, lying to their clients that the investment is performing well.

The solution: Do research before making a major cash investment. Check out your potential investment professional or banker with everyone from the Better Business Bureau to the Securities and Exchange Commission. Try to find referrals — is the person on the level? Look for warning signs, such as being given information that sounds vague or too good to be true. Be vigilant and realistic.

"Don't let greed overcome your good judgment," according to DailyFinance. "If your inner alarm bells are going off, listen to them and find another investment." Debt relief expert Freeman says that victims should be careful — implicate yourself in a Ponzi scheme, she says, and you could be charged with fraud.

12. Crowdfunding Scams

The scam: Crowdfunding is the newest way to raise donations for a special cause and a great way to donate money for a campaign you care about or to people in financial need. Websites like Kickstarter and GoFundMe have changed the way people look at fundraising in the digital space. But as with anything involving money and finances, scams have popped up.

In the last year, there have been at least three cases of people faking diseases such as cancer to solicit donations. Recently, a woman from Oklahoma managed to collect more than $3,000 in crowdfunding charity money after lying about suffering from terminal stomach cancer.

The solution: Trust is a tricky thing — it would almost seem inhuman to doubt a person seeking donations for cancer treatments. Still, you should proceed with caution anytime you don't feel right about handing over your money to a person or group. Do your research and try to find any information or feedback on the campaign. Donate carefully if you decide to give. If you are aware of a fraudulent or false crowdfunding campaign, notify the site involved and avoid getting taken.

From GoBankingRates.com: How to avoid these 12 scary money scams