TOP SCAMS	TIPS/WAYS TO AVOID
Grandparent scams. Fraudsters call and pretend they are a family member in need of help (ie arrested or ill) and urgently need money. They try to isolate their victims with fake reasons why the victim cannot consult with others. Some may even go so far as to have a third conspirator pose as a courier and go to a grandparent's home to pick up the money.	• Don't answer any emails or phone calls from unknown person. • Choose a "safe word" or "password" to share with that must be used in an emergency situation so they know it's you. • If you get a call or text from someone claiming to be a loved one but using an unfamiliar number, call or text the usual number that you use to reach that person to confirm they called. • Confirm emergency financial requests with other family members.
Romance scams. Fraudsters use new, fake relationships to steal people's money. These often start on social media or dating apps. The new love interest gains trust, then requests money for someone close to them. Scammers will ask for payment in ways that are harder to trace. such as gift cards and peer-to-peer services such as Venmo and Zelle. They also will extend an offer to help invest in cryptocurrency. FTC says the most significant dollar losses — more than 1/3 of losses to romance scams in 2022 — were in cryptocurrency.	• Talk to friends or family about a new love interest and pay attention if they're concerned. • Don't share any personal information with a love interest such as sernames, passwords or one-time codes that others can use to access your accounts or steal your identity. • If someone you've just met tells you to send money because they're in trouble or to receive a package, the FTC says you can bet it's a scam.
Cryptocurrency Scams. Investment-related scams are the most costly type of financial fraud. Scammers use cryptocurrencies because they don't have the same legal protections as credit or debit cards, and payments usually can't be reversed.	• Don't mix online dating and investment advice. If you meet someone on a dating site or app and they want to show you how to invest in crypto or ask you to send them crypto, it's most likely a scam. • A legitimate business or government entity will never email, text or message you on social media to ask for money; nor will they ever demand that you buy or pay with cryptocurrency. • Don't pay anyone who contacts you unexpectedly demanding payment with cryptocurrency.
Employment Scams. Scammers use enticing, hard-to-detect tactics to lure victims through interviews with a company that may seem legitimate. Then the fake employer sends a fake email to collect personal information, or says they're using a third-party, which is also fake, to do a background check. Once they have the target's personal identity information, it's an easy step to get into their bank account. Other job scams may promise guaranteed or easy income if you purchase a program they offer, or you'll see job opportunities that involve receiving or sending money to another account.	• Look up the name of the company or the person who's hiring you, plus the words "scam," "review" or "complaint." See if others say they've been scammed by that company or person. • Never click on a link from an unexpected text, email or social media. message, even if it seems to come from a company you know. • Don't ever pay a fee to get a job. If someone asks you to pay upfront for a job or says to buy cryptocurrency as part of your job, it's a scam.
Online Account Tax Scams. Swindlers pose as a "helpful" third party and offer to help create a taxpayer's IRS Online Account at IRS.gov. Third parties making these offers will try to steal a taxpayer's personal information. The criminal then sells this valuable data to other criminals, or uses it to file fraudulent tax returns, obtain loans, and open credit accounts.	• The only place individuals should go to create an IRS Online Account is IRS.gov. • DO NOT use third-party assistance, other than the approved IRS authentication process through IRS.gov, to create an IRS online account. • Don't store financial records and information in an email account. • See IRS Dirty Dozen Tax Scam List: https://www.irs.gov/newsroom/dirty-dozen.
Fake Check Scams. There's been a steep rise in the number of cashier and bank check scams. These involve other scams including lottery and inheritance scams; online auctions, classified listing, and overpayment scams; work-at-home employment scams, and secret shopper scams. In all of these cases, the scammer hopes to receive their payment before the fraudulent cashier's check is detected.	• Make sure the check was issued by a legitimate bank. Use FDIC BankFind Suite to locate FDIC-insured banking institutions in the United States. • Call the bank that supposedly issued the check to verify the check. Look up the phone number on the bank's official website and don't use the phone number printed on the check. Be aware that the bank may not confirm or talk to you. • Consider how and why you received the check. If someone you don't know initiated the payment, proceed cautiously. • Scammers often communicate via e-mail or text message. Their messages often have misspelled words and grammatical errors. • Look where the check was mailed from—if the postmark is not the same city/state as the issuing bank, it might be an indication the check is fake. Be especially cautious if it's from overseas. • Determine if the check is for the correct amount. Fake checks are often made out for more than the agreed upon amount. • Official checks usually contain watermarks, security threads, color-changing ink and other security features. While scammers are able to sometimes copy these security features, the quality is usually poor.

Learn more in Resources section of our website at: https://www.fmpierz.com/resources-education/