Most Common Scams in Orange County 2023-24

Romance Scam – Still the most popular scam in OC. Dollar losses are climbing as scam expands its reach. Scammer contacts victim via social media or dating site. After initial contact and building rapport, convinces victim he/she loves them and suggests meeting. Scammer asks victim to send money as his/her finances are frozen for some reason. Victim sends money to someone he/she believes loves them even though they have never met in person or often even spoken on the phone. This scam can go on for years while the perpetrator steals hundreds of thousands of dollars using an unlimited number of excuses for never meeting the victim. If you have never met someone no matter what they tell you, be suspicious. Never send money to someone you really don't know.

Investment Scam – This scam usually begins on social media or dating site. Scammer contacts you and builds rapport as an investment specialist. Scammer mentions an investment he/she has done with unbelievable returns. Will start with small dollar asks then send fake investment reports showing your gains. Sometimes scammer will also send you a little money to keep the lie going soon to be followed by a larger financial ask. Pretty soon the scam has taken tens or hundreds of thousands of dollars that are not recoverable.

QR Codes –Lurking behind a fake QR Code is the ability to drop malware into your smartphone and take all your personal and financial data. Be careful clicking on QR codes unless you know exactly what they are for. We are beginning to see more of these used in mail fraud cases for lower mortgage rates or quick HELOCs. Beware clicking on QR Codes as they could be the malware for your smarthphone.

Federal Agency Impersonation Calls – We are seeing more and more reports of unsolicited calls coming from what appear to be federal agencies or a high level of law enforcement asking for immediate payment for something you didn't do but are being threatened to pay. Threats include naming of children and grandchildren who will suffer if you do not pay or threats that you are being surveilled by someone outside your home. These are intended to scare the victim into forking over significant amounts of money – tens of thousands of dollars. Do not answer any call you did not initiate. Always go to the source for the actual phone number – never return a call or click on a site unless you know exactly who you are contacting. Federal agencies do not have the time or personnel to call you. And never give money to someone you don't know.

Technology Scams – Still the most common computer scams are the tech scams that suddenly flash and say your computer has a virus, call Microsoft or 'us' now. Close your computer, unplug it, do whatever you need to do to turn it off. Once it goes to sleep, the malware they are trying to download to steal your personal and financial information cannot download. Then contact a tech support service such as Geek Squad to check your computer for malware.

Amazon Scam -Another very common scam via text or email claiming someone is using your Amazon account to purchase an \$800 computer – call or click on this link to confirm your account information. These scams are so common but are still quite popular. Do not open any attachment or respond to any text or email unless you know for sure it is legit. Drag the email to junk or spam so it does not show up again.

USPS Text Scam – This scam is so popular that some even receive it in the Post Office parking lot thinking it could potentially be real. There is an issue with the package you have mailed through the US Postal Service. Click here or call this number to confirm the address and phone. Trust us, it's a scam!

Bottom line – Do not answer unsolicited calls. Do not open emails or attachments from unknown or unexpected sources. Never provide personal or financial information to anyone unless you know for sure who it is and what it is for. Trust your gut – we are rarely wrong when it comes to our body's natural reaction. Just hang up! And report these scams to law enforcement!

(Souce: Financial Fraud Unit Council on Aging - Southern California)