COMMON FRAUD TYPES

TACTIC: GIFT CARDS

Bad actors convince you to buy and send them gift cards. Often, this is presented as the only means to avoid losing social security benefits, jail time for tax issues, losing utilities, or falling behind on payments. It's made to seem like a very simple solution, and the fraudsters will urge you to take immediate action to avoid the dire consequences.

PREVENTION

Legitimate businesses or government entities will never require you to send them gift cards. If you receive a call, text, or email demanding this action, it is a scam. The bad actor urges you to take immediate action to discourage you from stopping to realize this is an odd request. Simply hang up or delete the text or email.

TACTIC: TECH SUPPORT

You're working on your computer and all of a sudden it happens: a pop-up warning you a virus has corrupted your system. Fortunately, this tech support company has caught it. And all you have to do is give them access to perform a "scan" of your computer. Unfortunately, what's really happening is they are working to get data. They may even ask you to log into your online banking so they can steal your login credentials.

PREVENTION

The messages in this scam are frightening, and you'll be tempted to take immediate action. But remember: no individual is actively monitoring your computer to protect you. So, if you get that pop-up message, ignore it. If you're worried the pop-up may be true, close it and contact your anti-virus provider directly or visit your local computer repair shop.

TACTIC: OVER-PAYMENT

This scam involves a bad actor posing as a legitimate business or buyer who "accidentally" overpays you. The fix seems simple: just send back the amount they overpaid. Sometimes, they'll ask for that overpayment back in gift cards. But here's the thing: the money, often a check, originally sent to you was never good. By the time the check comes back as bad, though, you've already sent the "overpayment" back. Or, the bad actors may have control of your online banking and show you the payment in your account. But as soon as you send the overpayment back, they transfer the original payment back out of your account.

PREVENTION

A legitimate company will never overpay you by hundreds or thousands of dollars. If you receive a check, bring it to your financial institution to confirm its legitimacy. Don't send any overpayment back until the check clears. And if you see the overpayment in your account, call your financial institution right away as your account may be compromised.

TACTIC: RELATIONSHIP BUILDING

Bad actors are very good at manipulating emotions. In fact, they're trained on it. They will convince victims of love or friendship so well that, when they ask for money, it seems completely natural…and safe. Or, they may try to convince you to invest in cryptocurrency. The manipulation will continue, and eventually, your account will dwindle. A tell-tale sign? You never meet the person. All your interactions are online or via text or calls.

PREVENTION

Bad actors know lonely individuals will do anything they can to maintain the relationship. Preventing this type of fraud means removing yourself from the situation and acting with a clear head. Talk to your financial institution if anyone starts asking for money. They will be able to guide you. Remember: you're eager to help your "friend", but they're eager to access your money.