INVESTIGATOR INSIGHT

Scam Artists – Gallery Of Deceit

"They told me there was a virus in my computer," reported Andrew to one of Kroll's Investigators during a recent consultation. This was how Andrew described the call he received from someone who identified himself as a technician for a global computer software developer offering to remove the dangerous virus. Andrew then allowed the caller to view his computer remotely and for the next six hours, the caller explored Andrew's computer and added icons to his computer screen. The cost: Andrew's credit card information so the "technician" could charge $120 for the services provided.

The next day, Andrew had an uneasy feeling about the whole experience. Calling Kroll to discuss the matter, he learned that his unexpected interaction with the caller was a scam. As it turned out, the technician was after his money, credit card number, information in his computer, or perhaps all of the above. Kroll's Investigator assisted Andrew in taking proactive measures to undo the damage done and reduce his risk of identity theft.

Unfortunately, this type of call is not uncommon. The scam artists play on human traits (fear, greed, gullibility, vanity, compassion, desperation, naivety) to paint a picture that is irresistible to the victim--a stunning work of art can capture the attention of virtually anyone.

To avoid becoming part of the scammer's next work of art, review the following information about common scams:

Computer Tech Scam

As in the example given above, this "artist" crafts a tale about being a representative of Microsoft or Windows and advises that your computer is infected with a dangerous virus. He then claims to be able to free your computer from the malware. Microsoft's website lists some of the things such a scammer can do if you fall for their scheme:

- Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords.
- Take control of your computer remotely and adjust settings to leave your computer vulnerable.
- Request credit card information so they can bill you for phony services.
- Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information there.

- If you get such a call, hang up. Do not pay for any service offered or provide any personal information to the caller.

Package Re-Shipping Scam

This scam artist paints a picture of rescue from financial struggle as the victim is often someone desperate for employment. The ruse: you are given a job where you accept shipments from various retailers and inspect the product before repackaging it and shipping it to the "employer."

During the hiring process the scammer obtains your personal information which is used not for employment reasons but to commit identity theft by applying for credit at online retailers. It is your credit the scammer uses to order the items sent to you and ultimately sent to him.

- Question a job that involves you receiving merchandise and sending it to another address.

Romance Scam

Hidden by the internet, this seedy scammer preys on the loneliness of another person. He sculpts an image of an upstanding and charming individual who has romantic feelings for the victim. It is not long before the scammer has reason to ask his sweetheart for money, exploiting the victim's trust. Victims can lose hundreds of thousands of dollars if they continue to believe the reasons given for needing a "temporary loan" which, of course, the scammer never intends to repay.

A cruel twist on this scam was reported by the Attorney General of North Carolina whose office received a complaint about a man who found a woman to befriend at the cemetery. She was visiting the grave of her husband. He "quickly wormed his way into her heart, her home and her bank account," according to the Attorney General.

To avoid a romance scam, the North Carolina Attorney General offers these tips:

- Remember, people aren't always who they claim to be.
- Never send or wire money to a stranger you meet online. Once the money has been wired, it is highly unlikely you will ever get it back.
- Never give out your personal information to someone you meet online, no matter what the circumstance or why they say they need it.

Overpayment Scheme

The maestro of this scam orchestrates a transaction of some sort between the victim and the scammer. The scenario may be that you allegedly won a lottery, they want to buy an item you are selling, or, perhaps they hired you as a "mystery shopper." For whatever the reason, they send a check to you written for more than the agreed upon amount and tell you to wire the additional funds to them or someone else. The excuse they give for sending the extra money relates to the transaction. For example, the scammer may tell you that the additional funds are to be used for:

- Paying taxes on the lottery winnings
- Shipping the item they purchased from you
- Paying for a background check for your new job

If you deposit the check, you are eventually notified that the check is not good. By that time, you've already wired money to the perpetrator. You've lost that money and you are held responsible for the bad check by your financial institution.

⬣ Never do business with someone who wants you to wire money to them after they have sent a check to you.

Tax-Related Phone Scam

The Internal Revenue Service (IRS) warns consumers of scam artists who've composed a sophisticated phone scam targeting taxpayers, including recent immigrants, across the country.

According to the IRS, victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer. If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license.

⬣ If you get such a call:

- Call the IRS at 800-829-1040 if you know you owe taxes or you think you might owe taxes
- Call the Treasury Inspector General for Tax Administration at 800-366-4484 if you know you don't owe taxes or have no reason to think that you owe any taxes