Week 1: How cyber scams are carried out and what to look for

You get a phone call, email, pop-up message or text from a phone number, company or address you don't recognize. Or, it's someone you recognize but you aren't expecting it and something seems off. What action should you take?

In today's world, where phishing, malware and other security threats are on the rise, we have to be ever so cautious. Cybercriminals continually evolve their techniques, making the lures harder to spot and threaten even the most perceptive targets.

We provide three examples in which all it took was one person to fall victim and significant amounts of money were lost. In each one, we provide the ways in which to identify the scam and how to go about avoiding such a scenario.

The fake tax debt scam

Scammers called by phone and advised the victim that she owed $4000 in tax debt. They were very demanding and hostile. In this case, the victim has English as her second language and was very worried as they threatened with police action and arrest. They demanded she go to a local store and purchase gift cards as a form of payment. She purchased $3000 iTunes, $500 Google Play, and $500 Steam cards. The scammers then sent WhatsApp messages to her requesting photos of the cards be sent, which she did. They then requested more money and more cards to which she declined and contacted family.

Signs this was a scam:

- The threats of arrest and request for unusual payment methods were the signs that this was a scam.
- Government agencies and any legitimate business will never threaten you with arrest, or demand immediate payment of a tax debt or fine with unusual payment methods like gift cards, Bitcoin, or pre-paid credit cards.

How to avoid this type of scam:

- Allow calls from unknown or unexpected callers to go to voice mail.
- Hang up the phone or delete the email - if you ever get a call or email claiming you will be arrested due to a tax debt. Do not call the number provided in the phone message or email you receive.

Remote access scams

In this example, a scammer called and was able to convince the victim that they in fact worked for the victim's local internet service provider and that his internet IP address had been compromised by hackers. The scammers convinced the victim to help them by sending money overseas in an effort to 'trap' the hackers. The scammers said they would deposit money into his savings account, then he was to use that money to send a MoneyGram overseas. They said it was important that he did no internet banking during this time for security

reasons. He did this several times until he became suspicious and checked his bank balances. The scammers had been getting cash advances on his credit card and depositing the money into his savings account.

Signs this was a scam:

- The victim was phoned out of the blue by a caller claiming to be from a large and trusted organization.
- The caller claimed the victim's computer was compromised. He also asked for account details and convinced the victim to send money overseas.

How to avoid this type of scam:

- Allow calls from unknown or unexpected callers to go to voice mail.
- Hang up on the caller.
- Refuse any request for remote access.
- Refuse to provide personal or bank account information to the caller.
- Refuse to transfer money from your account.

How an entire town fell victim to phishing

Back in 2019, the small town of Erie Colorado hired SEMA Construction to build a bridge. In October of that year, an unknown scammer completed an electronic form on the town's website requesting a change in how SEMA would receive payments for its work. Although town staff checked some of the information on the form for accuracy, they did not verify the authenticity of the submission with SEMA Construction; they accepted the form and updated the payment method. The town then processed two payments to SEMA for the work, totaling more than $1.01 million, except the accounts were never authorized by the construction company. Once the payments were in that account, the perpetrators of this fraud sent the money via wire transfer out of the country. The town is currently working with their insurance company and the FBI seeking reimbursement for the loss.

Signs this was a scam:

- The money was requested via the web site.
- It was requested the payments be made via wire transfer.

How to avoid this type of scam:

- Verify the form information by calling the company that you are sending payment to.

What to do if you are scammed

Cyber criminals are always thinking of new ways to fool people, so use caution anytime you're interacting online or via phone. If you fall for a cyber-scam (or think you may have), don't be embarrassed. You should turn off your computer, call the IT help desk immediately @ 1-800-373-7521 and report all relevant information about the incident as well notify the finance department. We will assess the situation and disable your account, assist in changing passwords, and rebuild your computer.