If Only They Used Their Talents for Good

As I write this, the Colonial Pipeline has begun transporting oil again after recovering from its recent ransomware attack. These types of attacks generally involve the introduction of a virus that blocks access to the files in a system (computer, network, etc.) until a ransom is paid. These and other types of scams have historically been aimed at individuals. In the last 18 months or so, I have noticed a sharp increase in the number of cold calls I receive – on some days they exceed 20 calls.

The ingenuity of scammers cannot be underestimated. I have often said to clients, "If only they used their talents for good…" Whether it is the imagination of the programmers creating viruses or the tenacity of the phone scammers, these skills could be used for good. Instead, we must remain cautious as scammers come up with creative new ways to separate us from our money. Ransomware is clearly a shakedown – overtly perpetrated for money. Others are more subtle.

Scams are ultimately intended to steal money, of course. Providing your credit card information over the phone or internet could open you up to unauthorized charges. Often, the objective of each contact (email, phone call, text, etc.) may be a small step toward the larger goal of what we broadly call identity theft. They may seek to open credit cards, file fraudulent tax returns, or access existing accounts. Doing so would usually require your name, date of birth, and Social Security number.

The number of possible ruses is endless, but here are some common ones:

• Consumer prepayment for services that are not performed, such as housework, medical equipment, title searches, timeshare sales, etc.

• The sweetheart scam and caregiver scam have swindlers develop a position of trust which allows them to gain control of the target's accounts. These prey on the target's desire for companionship.

• The grandchild scam takes advantage of compassion for family. This scam has someone phoning the target posing as or purporting to represent a relative – most often the grandchild – who is experiencing some crisis and is in urgent need of cash. Depending on the victim, the grandchild scam could be motivated by fear.

• Preying on fear is certainly the objective with IRS scams. I receive at least one call per day where a recorded message informs me that IRS agents are on the way to my house. The recording is not very convincing, but I suspect that it will improve with time. I have also received email from the IRS regarding personal tax issues. It is important to note that, according to IRS.gov, "The IRS doesn't contact taxpayers by email, text messages, or social media channels to request personal or financial information. This includes requests for PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts."[1] Further resources can be found on www.irs.gov. Once on the site, search for "phishing."

Phishing is a term used to describe the sending of emails claiming to be from reputable companies aimed at trying to get individuals to reveal personal information. The IRS scam involves spoofing, which is the act of making a communication (phone call, email, etc.) from an untrustworthy source appear as if it is from a trustworthy source. They can make an email appear as if it is from the IRS and use your fear to compel you to divulge personal information. A similar tactic has been used to gain access to personal computers. The target receives an email or phone call from someone posing as a recognizable technology company, such as HP or Microsoft, claiming that your computer has a virus. They offer to help you get rid of it by asking to you to go to a specific website and allow them to control your computer. Once access has been gained, they can then get your personal information.

How do you protect yourself? Securing your information begins with your securing and maintaining your network and devices. In addition to establishing passwords on your wireless network, computers, smartphones and applications, two-step authentication should be used wherever possible. Two-step authentication involves entering a password and then at least one other piece of validating information. This is often a key code that is sent via text message to the user's phone. Ensure all your PCs use antivirus software. Back up your data regularly.

Review your privacy settings on social media and be careful what information you share on social media. Some personal information can be inadvertently shared, including your address and birthdate. Further, answers to many common security questions may be easily found, including your mother's maiden name, favorite sports team, pet's name, etc.

Don't click on unknown links or open suspicious attachments. Opening an unknown link can unleash viruses. Don't fall victim to "your computer is infected" messages or messages making unrealistic threats or demands.

What do we do to protect you? We periodically receive spoofed emails from clients requesting cash. They generally involve an explanation for why the client cannot speak – too busy, travelling, medical reasons. Sometimes, they involve some small piece of accurate personal information. We will call you if we receive a suspicious email, regardless of the request. We do not provide or request personal information via email. We may request it verbally, by phone, if we need to verify your identity. All third-party bank wires require verbal confirmation and a signed Letter of Authorization. At times, clients are inconvenienced by various security measures, but such measures are in place to protect client assets.

Raymond James requires the entire staff to go through training on recognizing the signs of these types of scams. While sharing the particulars of that training would not be prudent, I will tell you that Raymond James tests our effectiveness by sending emails that should trigger our suspicion.

If you believe that your personal information has been compromised, you should call us and any other financial institution with whom you deal. Each firm has a process for placing additional safeguards on accounts.

Both Burke Financial Strategies and Raymond James consider the security of client accounts to be of the utmost importance. This information was largely gathered from materials created by Raymond James. If you would like more information, please let us know.

Sincerely,

Christopher M. Trainor

Christopher M. Trainor, CFP®
Financial Advisor

[1]https://www.irs.gov/privacy-disclosure/report-phishing