Social Engineering

Criminals understand that if we see an exciting Subject in an email like "Elvis Is Alive!" we just might click on it. They know that when we get a call from an angry person who says we owe money and they will turn our power off, we are frightened. The reason criminals are calling or emailing you is that they need your help to defraud you. If they didn't, they would not have to bother you.

To trust is fine but not to trust will keep you safe. Always validate who is calling or emailing you. In today's world, you must assume that someone knows enough about who you are, who your friends and family are that they might be able to fool you. Listen for the clues.

Clues

Sense of urgency—must act now
Anger, threats of harm—you did something wrong, you owe money or taxes.
Great opportunity – once in a life time opportunity, you are rich.
Must share personal information NOW!
Must send money to get money NOW!
Must do what they say NOW!

Be very wary of email attachments—They are a principle source of malicious software that can steal information from you.

Report any fraudulent calls or emails to your local police agency.

email@cfcpa.org

www.CFCPA.org

Central Florida Crime
Prevention Association
P.O. Box 432
Goldenrod, FL 32733

Central Florida Crime Prevention Association

Staying Ahead of Crime

The DNA of Fraud

Form 7-2016

What is the makeup of a fraudulent scheme? Here are a few clues you should be looking for.

Sense of Urgency

Did someone call or email you with something that requires immediate action on your part?

A threat against you or someone you know?

Are you being told that if you do not act, act now, someone will be harmed, maybe you or a family member? Threats like these often include false claims of debt, litigation, or arrest.

Is there an offer that sounds too good to be true?

Everyone wants to be a winner. Few are. When you have just been told that there is money just waiting for you, THINK FRAUD FIRST!

Responding to Fraud

Fraud, scams can be complex. But most depend on you trusting the individual at the other end of the phone or email. In today's open information society, it is easy for someone to gain a few facts and misrepresent themselves as someone you

should trust. A caller can claim to know you or a family member, claim to be the IRS or other government agency, even claim to be from your local police.

Social Media holds a wealth of information about almost everyone. Hacking of corporate and governmental databases has exposed even the most personal information about virtually everyone to misuse. Your job is to view every caller, every email, every representation as suspicious until proven otherwise.

A First Clue!

They want information! Things like your SSN, Drivers License Number, Credit Card Numbers or Bank Account numbers are worth money in the hands of any criminal. If someone asks for personal information, DO NOT GIVE IT.

A Better Clue!

Someone wants you to send money. The way they want you to send it is through wire transfer or money order. These are typically impossible to trace and a very convenient form for criminals to use to solicit funds from someone.

What to do

Never trust caller ID or the area code. Today, someone from any country in the world can call you using your local area code. They can even use your own phone number in your caller ID. End the call and then look up the number yourself, then call. This independent check will provide you the peace of mind. Validate the call.

NEVER click on a link in an email. Don't reply, close it. Look up the proper email and start a new email from you to the business or friend. Ask if the claims being made are true.