BEWARE: Criminals Want Your Money $

January 29, 2015 by Genevia Gee Fulbright, CPA, CGMA

If you have not already noticed, criminals are becoming more aggressive and sophisticated.

Signs of aggression

The other day I received a call from a distraught taxpayer (let's call her Mandy) stating that she might have made a grave mistake by releasing information to an aggressive shyster who was posing as an "IRS bully."

First of all, in my 20+ years as a professional advisor (including a short stint as an IRS Agent) I can assure you that IRS Agents work very diligently to avoid being characterized as a bully. They have a job to do and have to follow certain protocols.

Warning # 1 ~ If anyone leaves a voice message or tells you, within the first few minutes of your conversation, that you are going to go to jail and/or demands that you provide ANY confidential information, immediately ask for their full name, title, office location and most importantly their badge number.

If the person hangs up, you've saved yourself some headaches. Stay tuned because they might call back or try to use other tactics. Consider setting up a security or safe word system with your children or other family members that only legitimate callers are provided.

Do not release any personal data over the phone unless you initiate the call and the individual is authorized to receive this type of protected data.

Note, if the caller happens to be a legitimate IRS Agent returning your actual phone call and is threatening harsh action, take a message and call your CPA and/or Tax Attorney immediately.

Some of the rules

At a minimum IRS Agents have to follow certain protocols including:

- Immediate disclose to the Taxpayer the Agent's name, title and badge number
- No detailed voice messages allowed on machines or with others, to comply with disclosure rules
- Treating Taxpayers courteously
- Allowing a reasonable deadline for follow-up (rarely is IMMEDIATE action necessary for initial contact)

Sophisticated players

Welcome to the age of "Cyber Criminals" who are computer literate, sophisticated script writers, software developers and excellent recruiters. Checkout our Savvy Cybersecurity Quick Reference

These deviants spend their time training others to develop or acquire computer software capable of making multiple random, auto-dial, disturbing and threatening calls without any human interaction, other than to set up the system. The sheer volume of calls provides enough follow up responses and data to sell to keep them engaged and profitable.

Warning # 2 ~ Unless you've received an official IRS letter (hard-copy) PRIOR to voice contact and you have not asked them to call you, it is a scam and these shysters are looking for more victims.

If you have asked the IRS to call you following up to a written notice, pull out the letter when they call and ask them to provide you with a code or something from the notice to ensure you are actually speaking to a legitimate IRS Agent. Again, IRS Agents do NOT initiate phone calls without authorization from Taxpayers.

According to Raymond Dunkle, CPA, CFE, CFF the President of a firm, Red Flag Reporting, that specializes in helping organizations internationally deter and detect unethical activity in the workplace, "Implementing some simple procedures at home can help you avoid fraudsters from gaining access to your personal and financial data. Computers should always maintain up-to-date Security and fraud detection software, only use secure wi-fi, never give personal or financial information over the phone, be careful what you post on social websites, do not let individuals into your home that you have not scheduled to appointments and check all id for repair and other service providers that you have scheduled."

Although some criminals attempt strong-arm robberies for purses, wallets and other valuables the rise of more computer savvy criminals will continue and they will become more creative with how they gain access to your precious confidential data.

If you think that your confidential data has been compromised and you do not have LifeLock or a similar highly recommended service immediately:

- Contact your bank, brokerage house, credit card companies
- Make sure your computer is secure and virus scan protection is up-to-date and you only use a secure wi-fi or Internet connection
    - Then change all passwords for bank, brokerage house, credit cards, health data portal, newsletters, social media websites, email account access (home and work)

The IRS recommends that people can report incidents of attempted fraud to the Treasury Inspector General for Tax Administration (TIGTA) at 800-366-4484 via fax (202) 927-7018 or email phishing@irs.gov .

You can also file a complaint with the Federal Trade Commission at www.FTC.gov Add "IRS Telephone Scam" to the comments in your complaint.

Remember, the IRS will never initiate a phone call and request personal or financial information by email, texting or any social media. If you receive ANY emails that look suspicious do NOT open any attachments or click on any links in those emails.