

PROFESSIONAL FINANCIAL SERVICES, INC.

"DESIGNING AND PRESERVING WEALTH"

ONE PLAN AT A TIME

ROBERT E. TUCKER
PRESIDENT
Tel (703) 391-0299
Fax (703) 391-0277

10913 LAWYERS ROAD
RESTON, VIRGINIA 20191
e-mail: bobtucker@pfsinc.info
website: www.pfsinc1.com

Dear Client -

Last week I emailed you a discussion about being alert to SCAMS, and I sent you information about the first of nine scams.

As promised, here are two more:

THE GRANDPARENT SCAM:

The grandparent scam is a type of fraud in which a scammer impersonates a grandchild or another close family member who is supposedly in urgent trouble and needs money immediately.

Perpetrators acquire personal information about your grandchildren (or other relatives) through social media or by purchasing stolen data from cyber thieves. They then call using the acquired information to impersonate the victim's grandchild (or other relative) and request immediate financial assistance to resolve an emergency (e.g., accident that resulted in personal injury, arrest by law enforcement).

Typical characteristics include:

- The caller claims your grandchild has been in a car accident, arrested, injured, or stranded while traveling.
- They may pose as a police officer, attorney, doctor, or bail bondsman to make the story seem legitimate.
- They often beg the grandparent not to tell anyone, claiming the grandchild is embarrassed or that a lawyer or police officer instructed them to keep it confidential.
- The victim is pressured to send money immediately, often by wire transfer, gift cards, cryptocurrency, or cash sent by courier.
- Increasingly, scammers use AI-generated voice cloning to imitate the grandchild's voice, making the call sound convincing.

Securities offered through LPL Financial, Member FINRA/SIPC
Investment Advice offered through Professional Financial Services, Inc.,
a Registered Investment Advisor and separate entity from LPL Financial

How to avoid becoming a victim

- **Stay calm and resist pressure to act immediately.**
- **Hang up and call your grandchild or another family member using a phone number you already know-not one provided by the caller.**
- **Ask a personal question that only your real family member would know.**
- **Never send money or provide financial information based solely on an unexpected phone call.**
- **Be especially suspicious of requests for secrecy or payment by gift cards, wire transfers, or cryptocurrency.**

The best defense is to verify the emergency independently before sending any money. Legitimate family emergencies can withstand a few minutes spent confirming the facts.

THE COMPUTER TAKEOVER SCAM:

The computer takeover scam is a fraud in which scammers convince victims that their computer has a serious problem and then trick them into giving remote access to the device.

Common signs of the scam include:

- **You receive an unexpected pop-up, phone call, email, or text claiming your computer is infected with a virus or has been hacked.**
- **The scammer pretends to be from a well-known company such as Microsoft, Apple, or your internet service provider.**
- **They instruct you to install remote-access software so they can "fix" the problem.**
- **Once connected, they may steal passwords, financial information, or personal files, install malware, or lock your computer.**
- **They often demand payment for unnecessary or fake technical support services.**

The reality: Legitimate technology companies do not make unsolicited calls or display pop-ups asking for remote access to your computer.

How to protect yourself

- Never allow remote access to your computer unless you initiated the support request with a trusted company.
- If you see a suspicious pop-up, do not click on it. Close your browser or restart your computer if necessary.
- Never provide passwords, banking information, or payment details to unsolicited callers.
- Keep your operating system and antivirus software up to date.
- If you think you gave a scammer access, disconnect your computer from the internet, run a security scan, change your passwords from a different device, and contact your financial institutions if sensitive information may have been exposed.

A good rule to remember is: If someone unexpectedly contacts you claiming your computer has a problem and asks for remote access or payment, it's almost certainly a scam.

Don't get sucked in to them, and please feel free to share this information with colleagues, friends, and family.

Next week I'll send you two more!!! Hope it's useful to you.

Best personal regards,



Robert E. Tucker, CLU
Chartered Financial Consultant