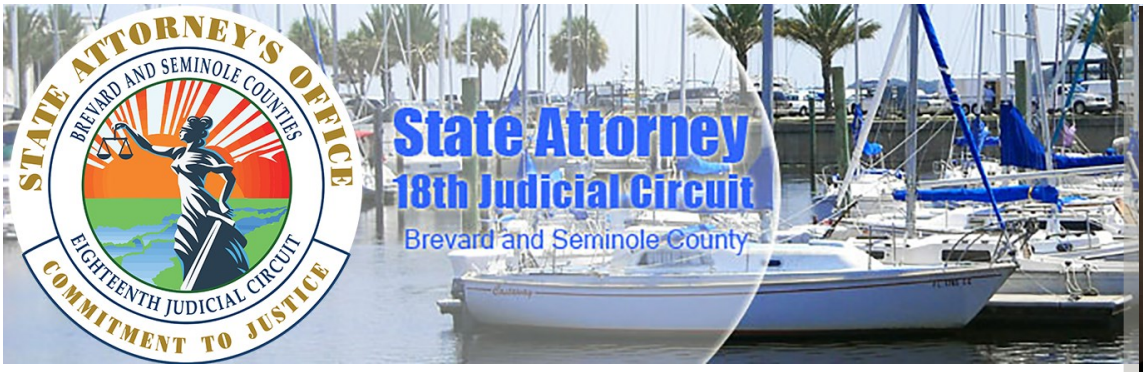
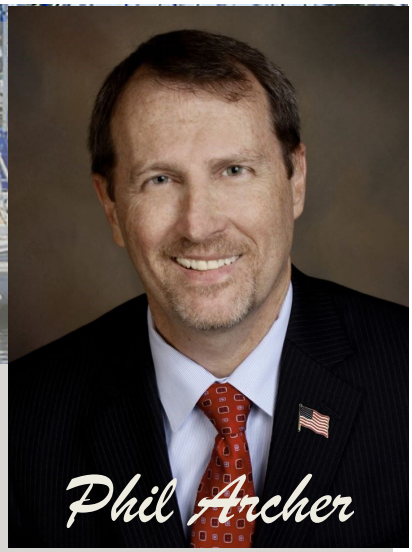




The Monthly Brief

Volume 11 Issue 3 March 2023

Home Energy Fraud

Inflation and soaring energy prices have us thinking about how much more it's going to cost for heating and cooling this year. Getting an email, a call, or a knock on your door with an offer to cut your utility bill dramatically might be tempting. But before you say "yes," know that scammers may be behind some of those offers. As you look for ways to improve your home's energy efficiency and cut costs, here's how to spot and avoid weather-related fraud this year:

• Be skeptical of products or services that promise drastic savings. Search online for the company or product name with words like "scam" or "complaint."

• Resist high-pressure door-to-door home improvement sales calls. The need to act fast is a red flag warning sign. Find a contractor who's licensed and reputable, and remember the Cooling-Off Rule.

• Get offers in writing and review them carefully before making any agreement or signing a contract. If the offer is good "today only" watch out. Look at the length of the contract or commitment, and if it involves early termination fees.

• Learn to spot scammers impersonating utility companies and threatening to shut off your service. One way to tell: anyone who asks you to pay with a gift card, cryptocurrency, money wire is a scammer.

Check to see if you qualify for help from the Low Income Home Assistance Energy Assistance Program (LIHEAP).

Learn more about ways to save energy with tips from the Federal Trade Commission.

*FTC

Follow Us On Facebook

Subscribe: philarcher@sa18.org

"Do Me A Favor" Scam

Most of us have a helpful disposition, we care. Crooks know it and use pleas for help as the bait in many of their scams. And now it's the "Can you do me a favor" scam.

It starts with a brief but very urgent message (email, text, social media) from someone you know, asking for a quick favor—run to the store and pick up some gift cards, they'll pay you later. The sender will usually include some reason why they can't do it

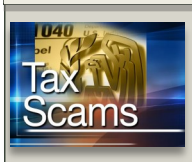
They may pose as a supervisor who needs the gift cards for an employee appreciation event. Another is a faith leader looking to quickly help a family in need, or a family member or friend. Usually the request is for specific gift cards and specific amounts, and you're asked to photo the front and back (exposing the PIN) and send the pictures. Gift cards are attractive to criminals—they are everywhere, aren't generally trackable and can be converted to cash in an instant. What you should do:

1) Stop. Anytime someone asks you to buy gift cards and share the numbers off the back, it's a scam. **2) Verify**. If you get a message like this, contact the person in a way you know to be legitimate and ask them if they sent it. **3) Report.** If you buy gift cards and later learn it was part of a scam, contact the retailer or card issuer immediately. If the funds weren't drained, you may be able to get some of your money back.

Learn more about these scams from the BBB and Detroit Free Press, and the FTC where you can also report the scam.

*AARP, BBB, FTC, DFP

Tax Scams Are Here



Tax season is here and so are tax scams. Messages offering tax rebates, huge refunds, and other benefits are showing up in Phishing emails, Smishing text messages, even ads sent by mail. If you click on a link to claim your "refund," you may expose yourself to identity theft or malware installed on your device.

If you're contacted about a tax rebate or refund: Never click on links, and don't share any personal information. Always use a website or phone number you know is real or call the IRS directly at 800-829-1040 to confirm.

You can check the status of any pending refund on the IRS official website IRS.gov. To report texts or emails claiming to be the IRS, forward a screenshot or the email as an attachment to phishing@irs.gov. If you clicked a link in a suspicious text or email and shared personal information, file a report at IdentityTheft.gov and get a customized recovery plan based on what information you shared.

Visit the IRS Guide to ID Theft. Get an IRS PIN number. Never give out your SSN or personal info to unsolicited contacts. Don't believe callers claiming to be with the IRS or any government agency asking for personal info or payments. Investigate any tax preparation service with the BBB, IRS or local business licensing offices. Protect all your accounts with strong passwords and multi-factor authentication. File a complaint with your local law enforcement and the Federal Trade Commission.

*IRS, FTC, CNBC, AAA,