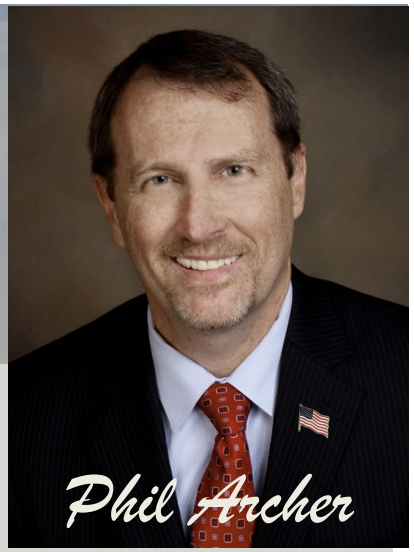
State Attorney
18th Judicial Circuit
Brevard and Seminole County
Saluting Service
Support Our Troops



The Monthly Brief

Volume 12 Issue 11 November 2024

Charity Check

Scam charities and crowdfunding campaigns use natural disasters to target those looking to help others in need. To combat this trend the BBB is offering tips along with a list of BBB Accredited Charities that are engaged in disaster relief activities.

Is the disaster appeal clear? The donation request should identify what disaster relief activities you are supporting. Don't assume what they do based solely on the group's name.

Does the charity already have a presence in the impacted area? If so they are more likely to deliver help quickly.

Is the charity established & experienced? These organizations will be able to provide help with greater speed and efficiency than a newly created effort.

If crowdfunding, do you know the groups organizers? Some sites vet postings after a disaster, others don't. Review the site's policies and procedures to find out. If in doubt, it is always safest to donate to people who you personally know and trust.

The BBB has evaluated and listed on their website several charities offering assistance to victims of hurricane disaster based on 20 standards of accountability. You'll find info identifying the charity, and specific disaster relief information.

Also visit BBB's Give.org & Charity Navigator to access free evaluative reports on other charities, along with helpful tips and information to help you to ensure your charitable giving goes where you want it to.

*Source BBB

Comments or Questions?

Subscribe: philarcher@sa18.org

Hacker Scam Continues

Last year the FBI warned about a hacker support scam and it's continued in 2024. It starts with a fake notification that appears to come from your bank or the government warning of a computer hack. This is known as a **"phantom hacker"** scam and the primary target is older adults, with more than half being seniors over 60.

How it works (watch a video): You get a call from someone who supposedly works for your bank. They claim a hacker from a foreign country is all over your account. Yikes! Then they say, "Hey, move your money to this 'safe' government account." But it's actually an account the scammer controls. **How to Avoid the Phantom Hacker Scam:**

Stay skeptical. If you get an unexpected email, text or pop-up warning about a computer breach, take a deep breath. It's probably a scam.

Check the source: Verify the message with the bank or agency directly before acting. Use a known phone number or website, not what's given in the suspicious message.

Never wire money: The U.S. government won't ask you to wire money to foreign accounts or buy gift cards. That's a scammer move every time.

If you've fallen victim, call your bank and then file an FBI report. If it happened to you, it happened to someone else. The more info the good guys have to go on, the more likely they are to catch the bad guys. For more info visit the FBI website.

*Source Komando.com, FBI

Medicare Open Enrollment Cons

Medicare open enrollment runs from Oct. to Dec. allowing participants to make changes to their coverage, and others to enroll. With the popularity of the program, scammers are targeting participants for fraud. AgingCare, FTC, AARP, and other media outlets are reporting on scams that are being used:

Phone calls from someone claiming to represent Medicare requesting your Medicare number and credit card information to sign you up for health coverage. Or asking you to confirm your Medicare number, personal info, banking details, or billing address as part of an account update. Some calls involve the false claim that signing up for Part D prescription coverage is required to maintain Medicare benefits. It's not, and totally optional coverage. Check out this informative video from Fox 10 News in Mobile AL

In another version, victims are called and told they are owed a Medicare refund. The call has potentially the biggest data payoff for a scammer, as they will often try to obtain your birth date, Social Security number, bank account and Medicare numbers.

Here are some tips to avoid these Medicare Scams:

1. Medicare will never phone you to sign up for plans or coverage. **2.** Medicare will never cold call and cannot ask for payment information over the phone or online. **3.** Never give out your personal info, Medicare number, banking details, or Social Security number to anyone you don't know or trust. For more info or questions visit Medicare or call 800-Medicare (633-4227). Or the AARP Hotline at **877-908-3360.**

* Source AARP, Komando.com, Medicare, AgingCare, FTC, Fox 10