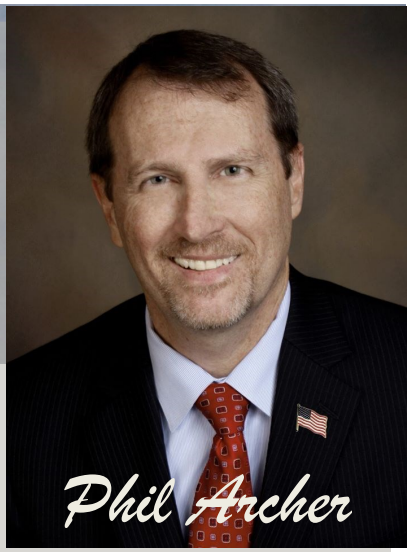
State Attorney
18th Judicial Circuit
Brevard and Seminole County

Saluting Service

The Monthly Brief

Volume 9 Issue 11 November 2021



Fake QR Codes

Companies use QR codes to point consumers to their apps, track packages, or view menus. But because these codes can't be read by the human eye, they have become a way for scammers to disguise malicious links

How it works: You receive an email, a direct message on social media, a text message, a flyer, or a piece of mail that includes a QR code. You are supposed to scan the code with your phone's camera, opening a link where you'll be prompted to enter personal info or login credentials. Sometimes the links are to payment apps or link to a malicious website or social media account. One victim told the BBB they received a fraudulent letter about student loan consolidation containing a QR code that linked to a fake student loan aid site.

How to Avoid QR Scams:

Don't open links from unsolicited sources or scan unknown QR codes, especially if they promise rewards, gifts or investment opportunities.

Verify the source. If a QR code appears to come from a reputable source, it's wise to double check. If it appears to come from a government agency, call first or visit their official website to confirm.

Use a Secure QR Scanner that can check the safety links before you open it. They can identify phishing scams, forced app downloads, and other dangerous links.

To learn more about how scammers use QR codes visit Security Intelligence or the BBB's website. *BBB

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Broadband Relief Scam

As the pandemic continues the need for reliable internet service has increased. A new government initiative called the Emergency Broadband Benefit Program provides a discount for broadband service to qualifying low-income/senior households. Discounts on certain devices are also available. But as we've said before, scammers follow the money and now the FCC is warning about a EBB based scam on social media.

To sign up for the real EBB Program, enrollment through a participating internet provider, or the FCC is required. Scammers are posting fraudulent ads on social media offering to help sign you up for the EBB program. All you need to do is pay a fee and provide your personal information. If you are offered access to the program through any means aside from the FCC and its listed providers, it's a scam

Here are some tips from the FTC to avoid EBB scams:

1. Only apply through the FCC, a participating provider, or by visiting the website GetEmergencyBroadband.org. If another company says it can sign you up for this program, check first to see if it's an approved provider**. 2. The EBB program is free** for those who qualify. Never pay to sign up for benefits. **3. Don't give your financial or personal information** to someone who calls, texts, or emails and says they're with the FCC. If you think a call or message could be real, be careful. **4. Call the Emergency Broadband Support Center** at 1-833-511-0311 to check any offers.

*FCC, Komando.com, GetEmergencyBroadband.org, AARP

Medicare Open Enrollment Cons

Medicare open enrollment begins at this time of year allowing participants to make changes to their coverage, and others to enroll. With the popularity of the program, scammers are targeting participants for fraud. The AARP highlighted some of the popular methods 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.

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