Fast Forward

Covid-19 Scams and How to Protect Yourself

Scams: There are several scams emerging that are targeting at-risk populations for Covid-19. These scams include, but are not limited to:

Check Scams: Calling to ask for banking or other sensitive information in order to process social security, retirement, or relief checks.

Treatment Scams: Selling fake cures, vaccines, and advice on treatment

Supply Scams: Creating fake shops, websites, social media accounts, and email addresses claiming to sell needed medical supplies, sanitizers, and medicine. Scammers pocket the money and never provide promised supplies

Provider Scams: Contact by phone or email from scammers pretending to be doctors and hospitals demanding payment for treatment of a friend or family member.

Charity Scams: Scammers soliciting donations for individuals, groups, and areas affected by Covid-19.

Phishing Scams: Scammers pose as health officials and send phishing emails to trick people to download malware or provide personal data or information.

App Scams: Creating fake apps designed to track the spread of Covid-19 to put malware on users' phone and gather personal information.

Investment Scams: Online promotions claiming products or services of publicly traded companies can prevent or detect Covid-19 and therefore their stock will dramatically increase in value.

Shopping and Prescription Scams: Scammers call seniors offering to pick up prescriptions or groceries for them. Money is left in envelopes outside of a senior's house for products that never arrive.

Fast Forward

How to Protect Yourself from Scams

Vaccines/Prevention Scams:

There isn't a vaccination for COVID-19 currently available, and there are no commercial products that can make you immune to the virus.

Beware of anyone trying to sell these types of products. If you are worried or have questions about vaccines, prevention techniques, etc., check the following links for more information:

1) National Institutes of Health (NIH): www.nih.gov
2) World Health Organization (WHO): www.who.int
3) Centers for Disease Control and Prevention (CDC): www.cdc.gov

Keep in mind: Doctors, hospitals, and medical professionals will never call and claim to delay treatment of any kind until a payment demand is met.

Investment and Check Scams:

You will not have to pay anything, confirm a bank account, or provide personal information to continue to receive your Social Security, Retirement, or any relief benefits.

The government will not call and ask for any sensitive information. Do not give any information over the phone.

Do not believe people calling or advertisements online claiming up-front investment for a pay-out later. Do your research before making any investments.

Charity Scams:

During this time of uncertainty, try and give to nationally recognized charities or local organizations you know to be legitimate and verified. Local food banks, shelters, and free clinics are always good places to start.

Charity Navigator: www.charitynavigator.org is a great resource to look up charities and find out their legitimacy.

Check how a charity wants the donation. If they insist on cash, gift cards, or wire transfers—they are likely not legitimate.

Fast Forward

Shopping and Prescription Scams:

There are volunteer groups and community members who are honest and helping seniors and those more vulnerable to Covid-19 shop and pick up items. Be cautious. Do not allow strangers into your home or give money to people you do not know to do shopping. If someone calls, ask what group they are representing (a church, food outreach, etc.). If you have a bad feeling, hang up and call the organization directly.

If you are having difficulty picking up food: please look on our senior page for resources available for seniors during this time.
http://www.columbiasharenet.org/helpful-resources

Keep in mind, pharmacies including CVS, Longs, and Walgreens offer prescription delivery. Check with your pharmacy and see about delivery options.

When shopping online, stick to places you are familiar with and know to be real. Do not click on ads that promise medical supplies or other products for a low price, or another gimmick. Check out the company. If it seems too good to be true, it probably is not legitimate! Right now, scammers are capitalizing on fear. Take a moment research. Does this appear to be true?

Email and Phone Calls:

Always be aware of who you are talking to on the phone and emailing.

- The best way to prevent phishing or scam emails is not to respond or open attachments from unknown senders.
- Do not open chain emails, or emails from someone that seems out of character. Call the sender and let them know you received something suspicious.
- Do not provide information to unknown people or groups by email. No one should contact you by email for your banking or any other information.

Phone Scams come in many varieties, they tend to make similar threats, promises, or ask you to pay money for a service.

1) The Government is not calling to confirm sensitive information. Do not give personal or banking information over the phone.
2) You will not be arrested- Scammers might say you will be arrested or fined if you do not pay a debt right away. The goal is to scare and bully you into paying. Hang

up, contact the police department (not 911) and let them know the number that called and what happened.

3) There's never a good reason to send cash or pay with a gift card. Scammers ask for money this way so it is harder for you to get your money back.
4) Pay to Win is not a prize. If you get a call that you've won something but you have to pay to receive it, it is most likely a scam.

How to stop phone scams:

1) Hang Up
2) Block the number if it calls repeatedly
3) Do not trust your caller ID. Scammers can make any number show up on caller ID. That is called spoofing.

For more information, or to report a call go to: www.ftc.gov/calls

App Scams

Avoid downloading apps that do not have lots of legitimate reviews or apps that claim to have information on "cures", vaccines, or other "click-bait" information.

Some map-based apps that trace the path of the virus could end up infecting a user's phone with a virus, the digital kind.
IT security company Lookout also found a 'Corona live 1.1' Android application which is a Trojanised version of the legitimate "corona live" app that allows users to get updated with data found on Johns Hopkins University's coronavirus tracker (Sangani, 2020).

Do not allow apps to access photos, media, files, device location, or contacts. Always think "Does this app need access to my photos/contacts/location? Why?" prior to granting any approval.

Sangani, Priyanka, and Anandi Chandrashekhar. "Fake Covid-19 Apps Fish in the Troubled Waters." *The Economic Times*, Economic Times, 23 Mar. 2020, economictimes.indiatimes.com/tech/internet/fake-covid-19-apps-fish-in-the-troubled-waters/articleshow/74766216.cms.