COVID-19 Scams and the Elderly

Coronavirus scams are becoming more ingenious every day. You may be aware of some of the pharming scams in the news lately where sites spoofing the World Health Organization or Johns Hopkins University are accessed through links that look like valid websites. These sites direct traffic to another site to capture personal information that can later be used to commit fraud and identity theft. They also install malware on your computer to gain access to all your information.

But seniors are particularly vulnerable during the coronavirus crisis. Here are 10 tips to help our seniors.

10 Tips For Seniors

Your bank can start helping seniors by passing along these 10 tips to help them become aware of scams:

1. Watch out for phishing scams. Phishing scams use fraudulent emails, texts, phone calls and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with, and NEVER give your password, account number or PIN to anyone.

2. Ignore offers for a COVID-19 vaccine, cure or treatment. Any medical breakthrough will not be first reported through unsolicited emails or online ads.

3. Rely on official sources for the most up-to-date information on COVID-19. Visit the websites from the Centers for Disease Control and Prevention and your state's health department to keep track of the latest developments.

4. Remember that the safest place for your money is in the bank. It's physically secure and it's federally insured. When you deposit your money at a bank, you get the comfort of knowing that your funds are secure and insured by the government. You don't have the same level of protection when your money is outside the banking system.

5. Do some research before making a donation. Be wary of any business, charity or individual requesting COVID-19-related payments or donations in cash, by wire transfer, gift card or through the mail.

6. Keep your computers and mobile devices up to date. Using the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

7. Recognize and avoid bogus website links. Cyber criminals embed malicious links to download malware onto devices or route users to bogus websites. Hover over suspicious links to view the actual URL where you will be routed. Fraudulent links are often disguised by simple changes in the URL. For example: www.ABC-Bank.com vs ABC_Bank.com.

8. Change your security settings to enable multi-factor authentication for accounts that support it. Multi-factor authentication—or MFA—is a second step to verify who you are, such as a text with a code.

9. Before you make any investments, remember the high potential for fraud right now. You should be wary of any company claiming the ability to prevent, detect or cure coronavirus. For information on how to avoid investment fraud, visit the website of the Securities and Exchange Commission.

10. Help others by reporting coronavirus scams. Visit the FBI's Internet Crime Complaint Center at ic3.gov to report suspected or confirmed scams. You can also stay up-to-date on the latest scams by visiting the FTC's coronavirus page at ftc.gov/coronavirus.

Information provided by American Bankers Association® (ABA)