Scams: What You Need to Know Presentation Summary Points

April 28, 2020

- Report scams to the **Maryland Attorney General's Office, Consumer Protection Division** at 1-888-743-0023.
- **Ploys Used by Scammers:** **Phishing** scams are designed to trick a person into revealing sensitive financial and personal information. **Spear Phishing** scams occur when the scammer has some information about you and he tricks you into revealing the rest of your information. Scammers **target their victims repeatedly** with different types of scams. Scammers **extort money from victims** by claiming the victim committed a crime and threatening to turn the victim over to the police for prosecution.
- **Telltale Signs of a Scam**: You are asked to **WIRE** money to someone you don't know. You are asked to pay using a **GREENDOT CARD** or **GIFT CARD**. A stranger sends you a **check** with instructions to **keep some of the money** and **send the rest to a stranger**. You are told to pay a **small** amount of money to win **BIG** money. A caller asks you to provide **personal information** over the phone and you ***didn't initiate*** the call.
- **Coronavirus Scams:** Bogus cures, vaccines and treatments being sold online. Scammers offer free COVID-19 test kits from Medicare or free "Senior Care Packages" containing highly sought-after hand sanitizer to get your Medicare ID number. Scammers call asking for your SSN and bank account information to process your stimulus check. Scammers ask for an advanced fee as a requirement for receiving your stimulus money, which isn't true.
- **Medicare Brace Scam**: Scammers claim that you're eligible for a **free back or knee brace** and then ask for your **Medicare ID number**. Medicare will be billed and may bill you for shipping. The crooks may send you a brace, even if you refused it before. **Don't accept delivery for a brace sent to you against your wishes. DON'T respond to tv or radio ads** urging you to call to get a free brace. **Report this scam** to the **Inspector General of the U.S. Dept of Health & Human Services.**
- **Medicare DNA Testing Scam**: Scammers offer **free DNA testing for cancer screenings for Medicare beneficiaries**. They need your Medicare ID number and maybe your social security number. They will swab inside your mouth and collect a DNA sample for testing. Scammers will bill Medicare and victims have reported not receiving any test results. Sharing your Medicare ID number and social security number with a stranger can lead to **fraud** and **medical identity theft**.
- **Social Security Scam**: The scammers say that your **Social Security Number (SSN)** has been **de-activated or your Social Security benefits have been suspended,** due to fraudulent activity. You will be asked to **confirm your SSN** over the telephone**.** To get a **new SSN or to re-activate your Social Security benefits**, the scammers will ask you to **pay a fee**. Report to the **SSA's Office of the Inspector General** at 1-800-269-0271 or **https://oig.ssa.gov/report** for online complaints.
- **IRS Scam**: The IRS is using **third party debt collectors** who may call, but the IRS and debt collector both **must send a letter first before they initiate telephone contact about back taxes.** Scammers

are sending out **bogus letters** claiming to be from the IRS about back taxes. Call the IRS directly to verify if a legitimate letter was sent to you.

- **Sweepstakes and Lottery Scams**: You receiving letter informing you that you have won a several million dollars in a sweepstakes. **The scammer may ask you to pay a processing fee or taxes before you can collect your "winnings."** ***Winning is free!*** **Never** have to **prepay taxes or pay administrative costs to receive sweepstakes or lottery winnings.**

- **Grandparent Scams**: The scammer claims your grandchild needs cash to get out of jail or for emergency medical bills. You are told to **wire money right away** and **to keep it a secret**. Call grandchild or other family members rather than send money. Protect yourself by using a **code word** that a stranger couldn't easily guess or **a fact** that only a family member would know to vet these calls, if you are unable to contact your grandchild to verify their safety.

- **Business Promotion Scam:** A scammer pretends to be from Comcast or other well-known national business with **a special promotion to lower your monthly bill for a two year period**. The scammer may know how much you currently pay and other account details, which makes it seem legitimate. You must **pay 6 months of service in advance** to lock in the lower rate for a two year period. You are instructed to pay using a gift card.

- **"Say Yes" Scam:** The scammer calls you and uses a question to elicit a "yes" response from you including "*Can you hear me?" or "Am I speaking with Mr. John Doe?"* The scammer records you saying "yes" and may try to use it as proof that you agreed to subscribe to a service or buy a product. Avoid saying "yes" on the phone. If you have said "yes," dispute any unauthorized activity that appears on your bank and credit card accounts immediately. In Maryland, you **can't enter into a contract to buy anything by simply saying "yes." You also have to sign paperwork agreeing to the purchase before it is a legally binding contract**.

- **Credit Card Fraud Alert Scam**: A scammer pretends to be calling from your credit card company about a **possible fraudulent purchase**. **The scammer has your credit card account information including your name and address**. When you confirm that you didn't make the purchase, the scammer tells you that he is going to open a fraud investigation. The scammer asks you to read the 3 digit security code on the back of your credit card, which now allows the scammer to make online purchases using your credit card. Never share any financial information with a caller when you didn't initiate the call.

- **Bank Account Temporarily Suspended Scam**: The scammer tells you that your bank account has been **temporarily suspended**. You must **confirm your social security number and bank account information immediately** to lift the suspension. Banks never call asking for your account information.

- **Tech Support Scam:** "This is Microsoft Tech Support. Your computer has a virus... we'll help you fix it." Scammers will sell you a software program to fix your computer. **Never give your computer password to a stranger over the phone**, which allows the scammer to take control of your computer. **Never allow** someone on the telephone to **download harmful software (spyware or a virus) onto your computer.** Spyware can gather sensitive information about you including any passwords to websites that you visit.

- **What to Do about Scam Calls: DON'T** answer the phone when an unfamiliar phone number appears on caller ID. **Hang up** the phone if you don't know the person on the phone. **DON'T talk** to scammers and **reveal any information about yourself** to these criminals. **Never give personal or financial information to anyone who calls or emails you**. Your bank, credit card company, or a government agency will **never ask** you for sensitive information by telephone or email. **Don't reply to email, text, or pop-up messages that ask for your personal or financial information**. **Guard your Medicare ID number** like you do your SSN and bank account information.