"Scams: What You Need to Know" Presentation

Summary Points (rev. 4.4.17)

A. Popular Scams to Steal Your Money

Counterfeit Check Scams: A scammer mails you a check with instructions to deposit it into your bank account and wire money to someone you don't know. The fake cashier checks are such good fakes that the bank may not always detect that the check is fake until days or weeks after you have deposited it into your account. You are liable to the bank for the amount of the check, once the bank learns that the check is fake. You will also lose whatever money you wire to a stranger. Scammers may also tell you to deposit fake checks in your account, withdraw some money and tell you to go to another bank to deposit the money in an account controlled by the scammer using a blank deposit slip.

Family Emergency/Grandparent Scams: A scammer pretends to be your grandchild who needs you to send money right away because your grandchild has been arrested or involved in an accident in a foreign country. You are usually told to wire money and instructed not to tell anyone. Call someone in your family to verify that your grandchild is okay rather than give money to these crooks. A stranger may also call to tell you that a family member has been kidnapped and you must pay ransom. The scammer may offer to send a messenger to your home to pick up the money.

Government Imposter Scams: A scammer claims that you owe back taxes to the IRS, so you must pay up immediately or risk being arrested. The IRS does <u>not</u> call people about back taxes—they send letters in the mail. A scammer will also claim that you must pay a fine immediately or be arrested since you missed jury duty. The Court Commissioner mails letters to people who miss jury service rather than call them. People who miss jury duty must explain why the failed to show up and they can reschedule a new jury duty date. If you are at least 70 years old, then you can be excused from jury duty if you request it.

Lottery and Sweepstakes Scams: Scammers will tell you that you won the lottery or a sweepstakes for big money, but you have to pay taxes or administrative fees upfront before they can send your winnings check. If you won a legitimate sweepstakes or lottery, taxes would be automatically deducted from any lottery or sweepstakes winnings before you receive your award. Scammers claim that you have won an all-expense paid cruise, but you have pay processing or administrative fees first. You shouldn't have to pay fees to win a prize; otherwise, it is likely a scam.

Charitable Solicitations: Scammers pretend to be asking for donations for a charity except they try to pressure you into making a donation without sending you any

material about the charity. Don't give donations over the phone to avoid being a victim of a scam. Never give your social security number when making charitable donations.

B. Phishing Scams

Definition and goals of scammers who use phishing: Phishing scams are when scammers try to trick us into giving up personal and financial information about ourselves. A scammer may claim to be calling from your bank and tell you that you need to confirm your personal information to re-open your temporarily suspended account. Banks, government agencies or other financial institutions never ask for sensitive information such as your social security number over the telephone or by email. Never give out personal information to a stranger who calls you or in response to an email.

Tech Support Scams: A scammer who claims to be from Microsoft tech support, will tell you that there is a virus on your computer and convince you to buy a software program from him to fix the problem. Then, the scammer will ask you for your computer password, so he can remotely take control of your computer and download the software. Tech Support does not call people alerting them about problems with their computers. If you give someone remote access to your computer, the scammer could actually download a virus onto your computer or install spyware that will allow him to get sensitive information about you from your computer. Don't be fooled by someone who claims there is a problem with your email account and tries to pressure you into paying them to fix the "problem."

Say Yes Scam: Scammers will attempt to trick you into answering "yes" to a question on the phone and record it: "Can you hear me? Did you vote in the last election? Are you the homeowner?" The concern is that scammers may have financial information of the people whom they are calling and they may try to use the person's recorded "yes" as basis for charging their credit card or checking account. ***In Maryland, you cannot agree to a purchase by being recorded saying "yes." You must also agree in writing to the purchase. If you have answered "yes" to anyone on the phone, monitor your accounts for unauthorized withdrawals or credit card charges.***

Credit Card Fraud Alert Scam: A scammer pretends to be calling from your credit card company about a possible fraudulent purchase. Once you confirm that you didn't make the purchase, the scammer will claim to open up a fraud investigation. The scammer may have your credit card number. Next, he needs to verify that your card isn't lost or stolen. He will ask you to read the 7 numbers listed on the back of your credit card. The first 4 digits are from your credit card number. The scammer wants the last 3 numbers—the 3 digit security code found on the back of your card. With this code, scammers can make online purchases using your credit card now. Never give out sensitive financial information over the telephone.

SOME SIGNS OF A SCAM

- Send a small amount of money to win BIG money.
- If they offer to send you money and you are told to keep some for yourself and send the rest elsewhere.
- If you are asked to WIRE money to someone you do not know.
- If you are asked to use a GREEN DOT card to pay for something or someone you do not know.
- If you are asked to provide PERSONAL INFORMATION over the phone and you did not initiate the call.
- If you are asked not to talk to others and/or to act quickly.
- If they want you to DONATE money, but refuse to send you information in the mail first.
- If it sounds too good to be true (it probably is!)

FREE Resources

Any questions about back taxes, contact the IRS at 1-800-829-1040.

Report scams to Maryland Attorney General's Office: 410-528-8662 or toll-free 1-888-743-0023 and to the Federal Trade Commission (FTC) at 1-877-FTC-HELP.

For identity theft concerns, contact the Maryland Attorney General's Identity Theft Unit, 410-576-6491.

If You're a Victim of a Scam:

If you sent a money wire to a scammer,	File a fraud complaint with Western Union (1-800-448-1492) or MoneyGram (1-800- 955-7777).
If the scam occurred on the internet or by email,	File a fraud complaint at www.ic3.gov.
If a scammer mailed scam letters to you,	Report suspected mail fraud to the U.S. Postal Service Inspector at 1-800-ASK-USPS (1-800-275-8777).

Report fraud to Medicare at 1-800-633-4227 or the Office of Inspector General in the U.S. Department of Health and Human Services at 1-800-447-8477.

Report social security scams to the Social Security Administration's Office of Inspector General at 1-800-269-0271.