Computer/Internet Scams

Phishing and **spoofing scams** can dupe older adults into giving out their personal financial information. Phishing scammers create authentic-looking emails, text messages, and/or internet pages to entice their victims into disclosing financial information such as credit card details, bank or credit card account numbers, Social Security numbers, Medicare numbers, etc.

Here are some examples:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

The messages may appear to be from organizations you do business with–such as your financial institution or your insurance company. They may even threaten to close your account or take other action if you don't respond.

The senders are "phishing" for your private account information so they can use it to commit fraud or identity theft against you.

Scammers disguise or "spoof" an email address to make it look like it is coming from someone you may know. For example, you may receive an email that looks like it is coming from a friend who needs money to deal with an emergency.

In another twist, scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associated with well-known companies. They say that they've detected viruses or other malware on your computer to trick you into giving them remote access or paying for software you don't need. These scammers take advantage of your reasonable concerns about viruses and other threats. They know that computer users have heard that it is important to install security software. But the purpose behind their elaborate scheme is not to protect your computer; instead, they are trying to install malware to steal passwords and account numbers.

Tips for avoiding computer or internet scams

Take precautions with your personal computer (PC) to reduce your risk of a computer/internet attack:

- Use trusted security software and make sure it's updated regularly.
- Do not email financial information or account numbers. Email is not a secure method of transmitting personal information.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can compromise your computer's security.

Be cautious about opening attachments and downloading files from emails, regardless of who sent them.

- Use passwords that will be hard for hackers to guess. For example, use a mix of numbers, symbols, and capital and lower-case letters instead of easily guessed words.
- Shut down your PC when you are not using it.
- Don't give control of your computer to a third party who calls you out of the blue.
- Do not rely on caller ID alone to authenticate a caller. Criminals spoof caller ID numbers. They may appear to be calling from a legitimate company or a local number, when they're not even in the same country as you.
- Online search results might not be the best way to find technical support or get a company's contact information. Scammers sometimes place online ads to convince you to call them. If you want tech support, look for a company's contact information on the software package or on your receipt.

For practical tips to help you guard against internet fraud, secure your computer, and protect your personal information, visit **OnGuardOnline.gov**. If you believe you are the victim of Internet crime, or if you are aware of an Internet crime, you can file a complaint with the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center at **ic3.gov.**

How to Respond to a Phishing Attack or a Tech Support Scam

Even if you use security software, chances are high that some questionable messages will get through. Some of these messages look very realistic. Here are some tips for protecting yourself.

- Do not open any message that comes from an unfamiliar source. If you open a suspicious message, delete it. Do not click on links or call telephone numbers provided in the message. Be wary about opening attachments.
- Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies do not ask for this information via email or text.
- If you're concerned about your account or need to reach an organization that you do business with, call the number on your financial statements or on the back of your credit card or in the telephone book. Do not call the telephone number that the caller or spoof website provides you!
- If you receive an email that looks like it is from a friend or relative asking you to send money, call them to verify that the email really came from them.

- If you think you might have downloaded malware from a scam tech support site, don't panic. Update or download legitimate security software and scan your computer. Follow the instructions of the security software to eliminate any problems. Change any passwords that you gave out. If you use those passwords for other accounts, change those passwords, too. If you paid for bogus services with a credit card, dispute the transactions with your credit card provider. Check your statements for any other charges you didn't make, and dispute those as well. For more information, go to **consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams**. If you believe you are the victim of Internet crime, or if you are aware of an Internet crime, you can file a complaint with the FBI's Internet Crime Complaint Center at **ic3.gov**.

Victims of phishing or tech support scams could become victims of identity theft. Act promptly to avoid financial loss or damage to your credit. You'll find more information and resources at the end of the following section on Identity Theft.