How to Protect Yourself from Some Common Scams

- Your bank and other financial institutions, the Social Security Administration, Medicare, and the IRS will never ask for personal information over the telephone, by email, or by text message. Do not provide or even confirm personal information. Never respond using contact information provided in the message. Ignore the message and confirm your account using trusted contact information.

- Messages announcing awards or freebies are scams or phishing attacks. Remember that "if it's too good to be true, it isn't!" Don't be intrigued by the promise of something free. That is just bait on the pointy end of a hook. Ignore the message. Never open an attachment or click on a hyperlink in a suspicious message!

- Did you receive a message that a package delivery is being attempted but they just need confirmation of the address or "a little more information." It may even look official from UPS or FedEx. But first ask yourself if were you expecting that delivery. If so, use the tracking link provided by the vendor when you ordered, or call using trusted contact information. Don't respond using contact information provided in the message.

- Did you receive notification of a (possibly large and unexpected) charge on your account, with a request for confirmation? Don't panic! First ask yourself, do you have a chargeable account with that vendor? If not, ignore the message. (If you order from Amazon, you have an Amazon login account, but products ordered are charged to your credit card, not to your Amazon account.) If you do have a chargeable account, check with the vendor using trusted contact information. If you are concerned that your bank or credit card account may have been compromised, confirm your balance and recent transactions with that institution, using trusted contact information. Don't respond using contact information provided in the message.

- Did you receive a message from a grandchild, relative, or acquaintance who is in trouble and asking for assistance? Don't panic! Tell them you'll call back and don't let the caller convince you to stay on the line. Don't believe a "grandchild" who asks you not to tell his or her parents. Don't call the jail or school or hospital using a number they provide. Look up the institution yourself. Call the person or institution using trusted contact information in order to confirm the situation. Call the parents anyway!

- Did you receive a message asking about your health and promising free advice or testing? Don't believe it, even if they seem to know a great deal about you already; perhaps even including your address, birthdate and Medicare number. These are commonly stolen and circulated among scammers, and do not prove the caller's legitimacy. The caller may be very persuasive and insistent, but if you agree to the test, you will be responsible for paying hundreds or thousands of dollars if your Medicare or other insurance refuses to do so (they know these scams). Call your own doctor or clinic if you need a test or advice.

- Did you receive a mysterious text message from someone not in your contacts? Perhaps it said, "Hey, we haven't talked in a while," or "I have your telephone number but I don't remember who it belongs to," or "Let's have coffee tomorrow, give me a call." Don't respond! Block the sender's number and delete the message.

- Did your computer screen freeze with a popup windows announcing that your system has been infected, or that a Trojan horse or a worm has been detected, and asking you to call the Apple or Microsoft customer support line? The message may look official with the appropriate company logo, and your computer really seems to be locked up. But DON'T PANIC! Turn off the power to your computer (pull the plug if necessary), wait a few minutes, then restore power and boot up again. If it happens a second time, repeat. Whatever you do, don't call the number provided for the "customer support" line. If you feel your computer may be compromised, take it to a reputable local computer repair center and ask them to check it for malware.

- For a suspicious email message, check the sender's address. If it's a nonsense string of letters and numbers, or if the domain address does not end in the company name dot com or dot org, don't trust it! For example, "@customersupport.microsoft.service.com" did not come from Microsoft! It came from someone calling themselves service.com.

- Did you receive an email from a friend or family with an unusual recommendation or request? Compare the sender's address *character-by-character* with what you know to be that contact's address. One character out of place is all it takes to know that your contact's email account has been hacked and is being used to send bogus messages to everyone in his or her address book, phishing for responses. Do not reply. Call your contact to let them know they have been hacked. If you this happens to you, reset your email account password immediately! Then warn all your contacts. Examine your email address book. If it's been compromised or emptied, your email host may have a way to restore a previous version. Otherwise you will have to recreate it from scratch.

- Keep the location bar visible in your browser at all times, and learn to pay attention to the URL for anything new or suspicious, or the result of a link from an unfamiliar source. Even if the website looks official, if the URL looks fishy or does not end in the company name dot com, dot org, or dot gov, don't trust it!

In general, remember that most scam attempts use *emotion* and *urgency* to stimulate a response. If you are triggered to respond quickly to an unexpected situation, pause, take a deep breath, and confirm the situation before acting. Examine the message and its sender carefully. Do you know them? Are you sure they are who they say they are? Find a way to confirm the situation without relying on information provided by the sender.

For more information about how to protect yourself from cybercrime, visit
https://milwaukeequakers.org/cybersecurity/