REMINDERS FOR SAFE COMPUTING PRACTICES

Avoid "Fix" Scams, such as:

* **Phone calls** where the caller claims there is a problem with your computer and offers to "fix" it.

* **Screen prompts** to update your computer or download software to scan and/or "fix" your computer. DO NOT CLICK on the offer (not even on the "X" to close the window, as the "X" button could contain code to launch a malware attack). Instead, restart your computer immediately.

Use caution when opening file attachments or when following any links contained in email or on the Web:

Malicious email may include enticing, believable subject lines and/or attachments related to banking, email error information (such as alleged non-deliverable email notices), invoice, IRS information, scanned files, shipment information, social media, etc. Malicious email may masquerade to come from a person or email address that is familiar to you. This is called "spoofing."

Don't take the bait!

Best Practice: Don't open any attachments or follow any links unless the email is verifiable. When verifying, call the person or vendor directly instead of replying to the email, since the reply-to address could be spoofed (see "Spoofed Reply-To Addresses" below). Here is a general safety rule: Instead of opening an attachment or clicking a link in an unverified email claiming it is from your bank, your social media account, etc., login to your account the standard way and check for any messages there. If the email is a promotional email, instead of opening attachments or following links within the email, access the vendor's website directly.

Spoofed Reply-To Addresses: If the reply-to address is spoofed, and you reply, it will go to the spoofed reply-to address instead of to your intended recipient, thus verifying your email address to the hacker or spammer. Alternatively, instead of using the "Reply" function, "Forward" a response to your intended recipient, which forces manual entry of their email address, thus eliminating a spoofed reply-to.

Links (aka “clickbait”): Links provided in email can direct users to malicious websites. Avoid following links without verifying they are legitimate. Alternatively, search the Internet for whatever content the link is supposed to access. Based on the search results, you can then access the content directly from the hosting website instead of clicking on the link provided in the email.

EXE File Attachments: As a general rule, never open an EXE file attachment. EXE files are executable programs and rarely appear in legitimate email.

PDF File Attachments: PDF files are commonly attached to emails. Again, know your sender. Don’t open anything suspicious. If you open a PDF file and it prompts you to click on any links, or provide user credentials, don’t do it.

ZIP File Attachments: ZIP files are “compressed” (or zipped up) and contain another file or files. Hackers commonly store their malware inside of ZIP files attached to email. Never open a ZIP file attachment without verifying it with the sender. Do this via a phone call, since replying to the email might send it to a spoofed reply-to address. If you are unable to verify, do not open the attachment and delete the email.

Avoid Personal Information Theft Scams:

* Avoid replying to email which requires you to enter personal information directly into an email or web page. Never provide a user ID or password in email.

* Avoid replying to text messages from any number or name asking you to reply with a confirmation code (or password, or any other personal information).

* Terminate phone calls where the caller poses as an authorized representative of a company and attempts to trick you into providing personal information. Be aware that scammers may change their Caller ID to disguise their identity.