INTERNET “Phishing” and Protecting yourself

Internet "Phishing" scams are one of the fastest growing frauds today. Phishing scams involve a bogus email, fax, letter, popup message, or text message that uses legitimate materials such as a company's website graphics and logos in an attempt to entice recipients to provide personal financial information. Many government agencies, businesses, financial institutions and credit card companies have seen their website graphics and logos used by fraudsters in phishing emails and on fraudulent websites.

How to Protect Yourself:

- Never respond to an unsolicited email, fax, letter, text, or pop-up message that is asking for detailed financial and personal information or click on the links or attachments in the message.
- Do not respond to a message – by email, letter, fax, text, pop up or phone call – that asks you to call a phone number to update your account or give your personal information to access a refund.
- Never give anyone your User Name or password.
- Do not give anyone you don’t know or trust access to your computer.
- Never give out your PIN by phone, mail, or email or by any other means.

For more information and helpful links you can go to: www.onguardonline.gov