INFORMATION, NEWS, AND SUPPORT
Information Security Shared Services

4th Edition
October 2016

Cyber Security Bulletin

What is Phishing?

Phishing is a ***fake email*** designed by cybercriminals and scammers to collect personal information for fraudulent purposes. The fake email is designed to appear as if it originated from a reputable brand, your employer, or ***someone you know***.

Malicious Links: The scammer's goal is to take control of your machine or acquire your personal information with malicious intent. Some emails will contain a link to a site that *looks exactly like a website that you trust*, such as your online banking provider or social networks and enables them to steal your data as you enter it. Some of the sites spoofed most regularly include *PayPal, eBay, Yahoo! and MSN*, as well, as financial institutions.

Malicious Attachments: The scammer's goal is to launch an attack by emailing you an infected file. *Opening the attachment will compromise your system* and, potentially, gives the attacker control of your machine.

Scam Artist: Other phishing emails simply try to get you to reply to the email with your bank or credit card information. A Scam Artist will attempt to trick you by stating you have won the lottery, someone left you a trust fund, or you need to update your bank information, but will *first say they need a payment for their services*, scamming you out of your money.

4 tips to protect yourself from phishing

1) **AVOID GENERIC EMAILS:** Fraudulent emails are often not personalized and begin with "Dear Sir/Madam." Be suspicious of email like this.

2) **AVOID SCARE TACTICS:** Scammers like to use a sense of urgency with phishing emails; threatening to disable an account or some type of legal action. Do not get pressured into providing sensitive information. Contact the merchant directly to confirm validity.

3) **NEVER REPLY:** If you are suspicious of an email, do not reply with any personal information. Also, do not request to unsubscribe as this will only confirm to the scammer that it is an active email. Simply mark as junk and delete.

4) **DO NOT OPEN ATTACHMENTS OR LINKS:** Attachments and links in phishing emails are often used by cybercriminals to compromise your computer. If it looks suspicious, it is best to delete or mark as junk mail.

Virginia's Community Colleges

VIRGINIA WESTERN
Celebrating 50 Years