How to Identify Phishing Emails

Summary: The most common type of cyberattack that many individuals encounter is known as phishing. Phishing is one of many type of manipulating methods used by cybercriminals to send malicious emails disguised as legitimate sources. This type of threat is used to retrieve sensitive information and steal user's data. This article will help you avoid potential phishing scams.

Step 1: Always check sender name and email for any inconsistencies and grammatical errors.

Step 2: In the body of email, look for immediate call to action, deadlines and urgency verbiage.

Step 3: Scan email for login, debit/credit card, password request and other sensitive information.

Step 4: Hover (place mouse over link for 2-3 second without clicking) over links to check for shorten URL's and altered links.

Step 5: Beware of suspicious/unexpected attachments – scan for malware.
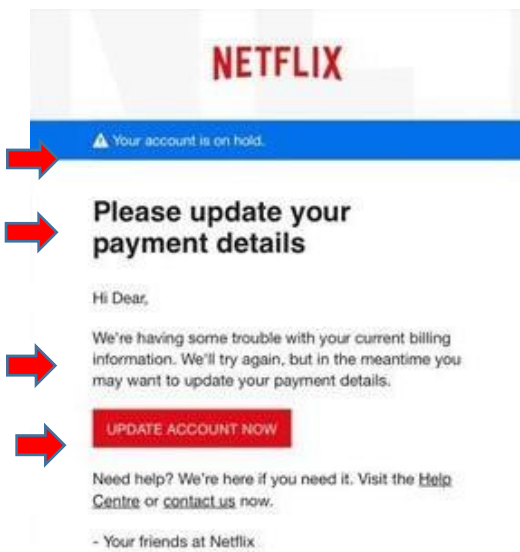
Step 6: Look for generic greetings, "Dear customer," "Dear airmen."

Step 7: Lookout for emails that claim there's a problem with payment, card, billing, login, etc.

Step 8: Recognize a poorly written email – grammatical errors, misspelling and incorrect formatting.

Example below of a phishing email and things to look for:

Things Phishy About This Email:

1. Immediate call to action requesting payment.
2. Generic greeting
3. A direct link provided to collect payment details.
4. Grammatical error – the word center was spelled "centre" British spelling for a U.S based company

Contact Information: DAF_Cybersecurity_Awareness@us.af.mil

TIPS:

1. Popular streaming services are now vulnerable for cyberattacks. Make sure you're checking domain names and submitting payments and inquires through direct site.
2. Netflix will NEVER ask you to enter personal payment information through email.
3. If you receive a suspicious email from them immediately forward to phishing@netflix.com then delete email.

Please report any suspected phishing emails to your security team or cybersecurity liaison.

Resource:

Federal Trade Commission, "Netflix phishing scam: Don't take the bait," 2018