The holiday season is upon us for family, friends, and … phishing?

December 2, 2019

This festive time of year is when many cyber thieves try to trick you with holiday-themed email scams. These **phishing scams are professional-looking emails that** attempt to steal your personal information (such as login password, bank account, or credit card). The emails generally look authentic and appear to come from a valid organization (like WVNET or your bank). They may even include a "helpful" link to a website for your convenience.

Some phishing examples from previous holiday seasons include:

From "Amazon": Enter your username and password to receive a "free" $100 Amazon gift card. Unfortunately, the webpage captures your login credentials and installs harmful software (known as malware) on your computer.

From "PayPal": You are "notified" that a fraudulent charge has been posted to your PayPal account. Just click on the link, enter your credit card number, and the charge will be cancelled. Unfortunately, you will now begin to see other holiday surprises appear on your credit card statement.

From "The IRS": You receive a threatening email from the IRS about unpaid taxes, lawsuits, arrest warrants, etc. You have to enter your Social Security Number and birthdate to check the status of your tax payments. You have also unknowingly become a victim of identity theft.

Keep the holiday season a happy and relaxing time. Here are some general tips to help you avoid falling for these online con artists:

1. Don't get pressured into providing sensitive information. Phishers like to use **scare tactics**, and may threaten to cancel an account or block a delivery until you provide the desired personal information.

2. Watch out for **generic-looking requests** for information. Fraudulent emails are rarely personalized.

3. Don't open unexpected files or pictures that are sent to you from "friends." Phishers can make it look like an email is coming from an address you trust (known as **spoofing**), with attachments that launch harmful software when opened.

4. Never click on a website link include in an email, even if it looks trustworthy. Instead, open a new browser window and **type the URL address yourself** into the address bar. Confirm that the website is secure (http**S**□ before entering confidential or financial information.

5. Finally, **if it looks suspicious**, even if you know the source, it's best to **delete it**.

Remember, offers that appear too good to be true are just that – not true. Also, when was the last time something good arrived via email? When in doubt, throw it out.

So, enjoy the holiday surprises while avoiding these seasonal nightmares.

– Carl R. Powell, Ph.D.
Director, WVNET