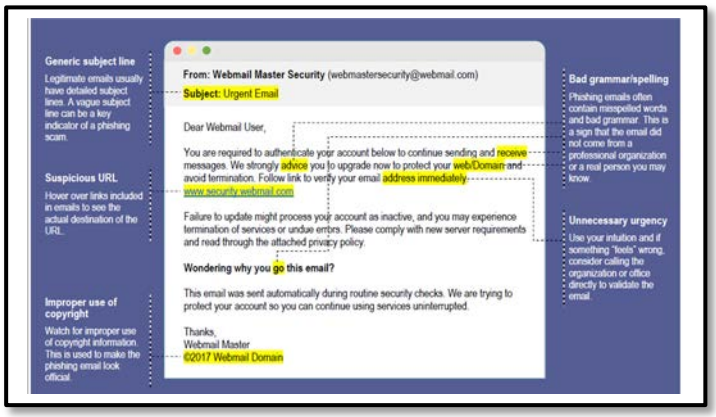
CTPAT ALERT

Cybersecurity: Don't Take the Bait: How to Spot a Phish

Last Updated: October 10, 2020

To All CTPAT Members - October is National Cybersecurity Awareness Month, so we'd like to continue to raise awareness about the importance of cybersecurity, ensuring that all CTPAT Members have the resources they need to be safer and more secure online. The purpose of this CTPAT Bulletin is to raise awareness about phishing attacks via email and how to stop them.

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Like fishing, "phishing" involves a fisher (the scammer) who tries to "hook" an unsuspecting user with bait (a message).



The good news is that you have the power to throw these phish back! Here are some tips to avoid succumbing to the bait and compromising your company's data and networks:

A. Be Cautious.

Remember the old warning about not talking to strangers? It goes double on the internet, since anyone can pretend to be someone else. An email from an exciting "new friend" could actually be a trick. Simply put, do not engage with suspicious email. This is an example of what attackers may email or text when phishing for sensitive information:

> "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."

B. Scan the message for these five indicators of a phishing email:

1. Generic subject lines such as "Hello Bank Customer".
2. Suspicious URL. Ensure that URLs begin with "https." The "s" indicates encryption is enabled to protect users' information. Also, avoid clicking on hyperlinks in emails and hover over links to verify authenticity.
3. Improper use of copyright.
4. Bad grammar/spelling.
5. Unnecessary urgency. Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy.

Hackers may also pose as senior managers and send very convincing phishing emails to subordinate employees that instruct them to send money, click on a link, or take some other action. Train employees to hit the pause button and consult with management to confirm the legitimacy of the unusual or suspicious request.

CTPAT ALERT

Cybersecurity: Don't Take the Bait: How to Spot a Phish

Last Updated: October 10, 2020

C. Practice good cyber habits:

1. Reboot daily which will install the patches to protect your equipment.
2. Do not open unsolicited emails, attachments, or links.
3. If you are concerned about the legitimacy of an email, call the company directly.
4. Follow your company's Cybersecurity Policies and Rules of Behavior and the CTPAT program's cybersecurity requirements and recommendations.

Report All Suspicious Emails and Spam

Please see CTPAT's Presentation on Social Engineering - Phishing on CBP' YouTube Channel
https://youtu.be/TeaqH9riVd4

The Cybersecurity and Infrastructure Security Agency (CISA) has several cybersecurity resources on its website. Please use these resources and share them with your stakeholders throughout the year to encourage a strong, cybersecurity posture. These materials are free and may be modified to meet your needs. They can be found here: https://www.cisa.gov/publication/national-cybersecurity-awareness-month-publications

They include a series of Tip Sheets on topics such as:

Social Media Cybersecurity Tip Sheet – With every social media account you sign up for, every picture you post, and status you update, you are sharing information about yourself with the world. Take these simple steps to connect with confidence and safely navigate the social media world.

Multi-factor Authentication Tip Sheet – Security breaches, stolen data, and identity theft are more prevalent than ever. We encourage Members to use multi-factor authentication. This technology may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email, or text containing a code.

Cybersecurity While Traveling Tip Sheet – In a world where we are constantly connected, cybersecurity cannot be limited to the home or office. When you're traveling— whether domestic or international—it is always important to practice safe online behavior and take proactive steps to secure Internet-enabled devices. The more we travel, the more we are at risk for cyberattacks. This document contains tips to connect with confidence while on the go.

CTPAT Appreciates Your Continued Efforts to Secure the International Supply Chain.

CTPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW Washington, DC 20229