Cybersecurity 101

A National Cybersecurity Awareness Month message,
brought to you by the Division of Information Security

Don't Get Hooked! *Phishing and how to avoid it*

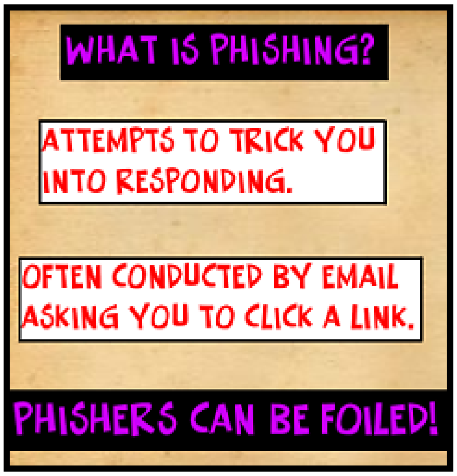
In an August 2014 incident reported by Reuters, a hacking group sent 150,000 emails targeting JP Morgan Chase banking customers. The email, which looked like a legitimate message from the bank, instructed recipients to click a link to a webpage and enter their online banking credentials—which were likely sent to the attackers. However, even if victims did not enter their information, the webpage would attempt to install a virus that steals banking information. This sort of attack is known as phishing and can result in identity theft, fraudulent charges, and stolen sensitive information.

At home or the office, phishing happens more often than you think. Be suspicious of any email with urgent requests for personal information.

Don't trust offers that seem too good to be true.

What is Phishing?

Phishing is a form of cyber attack where targets receive an email that looks like a legitimate message from a trusted institution, such as a bank or government office. These emails trick recipients into responding with private information (such as names, Social Security numbers, or account passwords), or entering personal information into a web form.



WHAT IS PHISHING?

ATTEMPTS TO TRICK YOU INTO RESPONDING.

OFTEN CONDUCTED BY EMAIL ASKING YOU TO CLICK A LINK.

PHISHERS CAN BE FOILED!

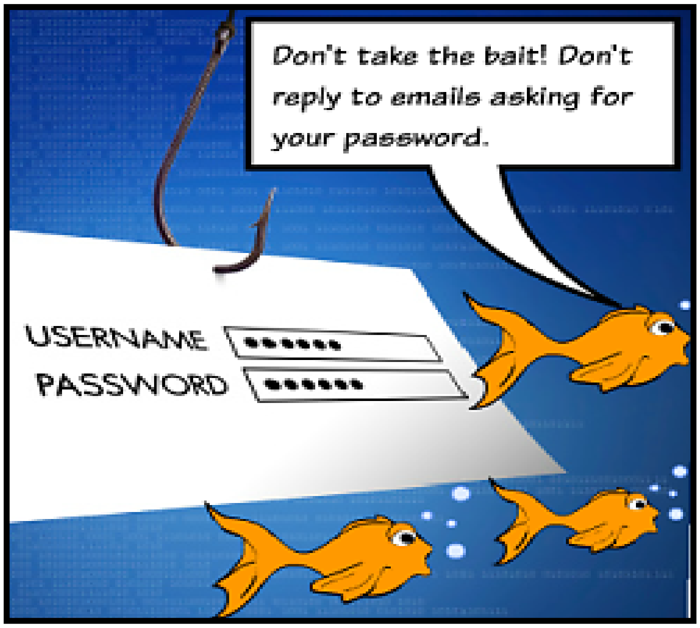
Types of Phishing

Phishing – messages sent to a large group of unrelated people

Spear phishing – messages sent to specific targeted individuals (likely within the same organization)

Phishing can come from anywhere. Beware of phone phishing schemes. Do not divulge personal information over the phone unless you initiate the call. Be cautious of emails that ask you to call a phone number to update your account information.

If you're concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.


Don't take the bait! Don't reply to emails asking for your password.
USERNAME
PASSWORD

CYBERSECURITY 101

A National Cybersecurity Awareness Month message,
brought to you by the Division of Information Security

How can I recognize phishing?

Here are some “red flags” that might indicate a phishing scam:

- unknown sender
- unexpected or unsolicited email
- requests for personal information
- spelling or grammar mistakes
- odd or generic subject lines
- unusual greetings
- unfamiliar or suspicious-looking websites and links
- references to current events

Always be cautious when encountering phishers. They are out to get your information quickly using sneaky and dishonest tactics.

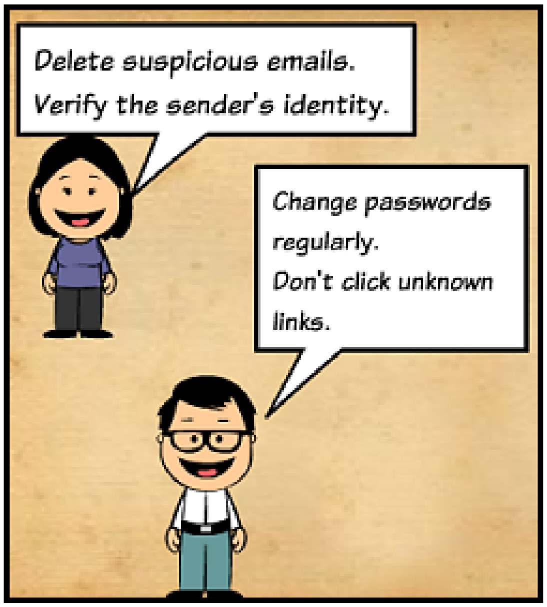
Avoid phishing: DOs and DON’Ts

DO...

…delete suspicious emails.
…verify the sender’s identity by calling the organization using a legitimate phone number.
…verify website addresses are spelled correctly before clicking.
…ensure website addresses contain https:// when sending information.
…report suspicious emails to your Area Information Systems Security Officer (ISSO). See http://home.ihs.gov/security/index.cfm?module=dsp_dis_sec_contacts.
…visit http://stopthinkconnect.org for more Internet safety tips.

DON’T...

…open unsolicited emails from senders you don’t recognize.
…reply to suspicious emails.
…give out personal information or login details in emails or suspicious web forms.
…send unencrypted sensitive information over the Internet.
…click links or download attachments without verifying the sender’s identity.


Delete suspicious emails.
Verify the sender's identity.
Change passwords regularly.
Don't click unknown links.

Be on the lookout for phishers. They can be anywhere and phish day or night.

October
National Cyber Security Awareness Month
staysafeonline.org

IF YOU THINK YOU’VE BEEN PHISHED, immediately contact your Area ISSO or HQ_OITSecurity@ihs.gov, check your accounts for fraudulent activity, scan your computer for viruses, and change your passwords.