Don't Catch that Phish – How to Not Become a Victim

STOP | THINK
CONNECT™

1. WHAT IS A PHISHING ATTACK?

- A phishing attack is designed to obtain sensitive information, generally through elicitation of the recipient or information stealing malware. The phishing communication ("phish") may be in the form of an e-mail, text message, instant message, or social networking message. Your personal or work accounts may be targeted by the attacker. You may become a victim of the attack if you do what the attacker wants you to do (e.g., sending information, opening a malicious attachment, or running a malicious file). In so doing, you may be deceived into trusting the sender or you may be motivated to respond or act, falling prey to the phishing attack.
- Phishing attacks are not necessarily random. You may be targeted specifically because of your position, your organization, who you know, what you know, or what you have access to (or what you can find out). The motivations behind phishing attacks may include financial gain, intellectual property theft (e.g., trade secrets, confidential know-how, and patentable inventions), obtaining business information (e.g., competitive information), revenge, blackmail, and political or social beliefs and ideologies. Victims who fall for phishing attacks may trust the sender or may be motivated by something in the message (e.g., reputation, goodwill, incentives, etc.).

2. HOW CAN YOU IDENTIFY THE PHISH? (ONE OR MORE OF THE FOLLOWING MAY APPLY.)

- Sensitive information is requested (e.g., login credentials, intellectual property, business information, personally identifiable information-financial, healthcare, or otherwise).
- Motivates the person to respond (e.g., job requirement, monetary incentive, blackmail attempt, etc.) or otherwise evoke trust.
- Conveys a sense of urgency (e.g., 24 hours to respond).
- Seemingly originates from a trusted person or company you may know (but the originating IP address may not be associated with that person or company).
- Seemingly originates from a legitimate company.
- Links to a malicious website, but the text or graphics may appear legitimate (hovering over the link may reveal the real site, which differs from what is shown).
- Contains or links to an unusual attachment (especially in a file format which you might not normally receive, such as .exe, .com, .zip, .bat, etc.).
- Contains bad spelling or bad grammar.
- More information can be found on the US-CERT website.

3. WHAT TO DO ABOUT THE PHISH, ONCE YOU HAVE IDENTIFIED IT?

- Follow organizational policies and procedures, such as contacting your help desk.
- Ignore unusual attachments, links, and messages.
- Places to report the phish include the Internet Crime Complaint Center and the FTC.

HIMSS transforming health through IT™

NATIONAL CYBERSECURITY ALLIANCE