February 2018

**Phishing**

Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information via electronic communication by impersonating a trustworthy source. For example, an individual may receive an e-mail or text message informing the individual that their password may have been hacked. The phishing email or text may then instruct the individual to click on a link to reset their password. In many instances, the link will direct the individual to a website impersonating an organization's real web site (e.g., bank, government agency, email service, retail site) and ask for the individual's login credentials (username and password). Once entered into the fake website, the third party that initiated the phishing attack will have the individual's login credentials for that site and can begin other malicious activity such as looking for sensitive information or using the individual's email contact list to send more phishing attacks. Alternatively, rather than capture login credentials, the link on the phishing message may download malicious software on to the individual's computer. Phishing messages could also include attachments, such as a spreadsheet or document, containing malicious software that executes when such attachments are opened. Phishing is one of the primary methods used to distribute malicious software, including ransomware.

Individuals must remain vigilant in their efforts to detect and not fall prey to phishing attacks because these attacks are becoming more sophisticated and harder to detect. Phishing attacks take advantage of popular holidays by impersonating messages from shipping vendors and ecommerce sites. Similarly, phishing attacks regarding tax refunds are common during tax season (March and April). A specific type of phishing attack, known as spear phishing, targets specific individuals within an organization. For example, a spear phishing attack could target an individual in the IT, accounting or finance department of an organization by impersonating the individual's supervisor and directing the individual to a malicious website or to download a file containing a malicious program. One of the primary methods of combating phishing attacks of all kinds is through user awareness. OCR included information on cybersecurity training and awareness programs in its July 2017 newsletter.[1]

Tips to avoid becoming a victim of a phishing attack include:

- Be wary of unsolicited third party messages seeking information. If you are suspicious of an unsolicited message, call the business or person that sent the message to verify that they sent it and that the request is legitimate.

[1] https://www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf

- Be wary of messages even from recognized sources. Messages from co-workers or a supervisor as well as messages from close relatives or friends could be sent from hacked accounts used to send phishing messages.
- Be cautious when responding to messages sent by third parties. Contact information listed in phishing messages such as email addresses, web sites, and phone numbers could redirect you to the malicious party that sent the phishing message. When verifying the contents of a message, use known good contact information or, for a business, the contact information provided on its web site.
- Be wary of clicking on links or downloading attachments from unsolicited messages. Phishing messages could include links directing people to malicious web sites or attachments that execute malicious software when opened.
- Be wary of even official looking messages and links. Phishing messages may direct you to fake web sites mimicking real websites using web site names that appear to be official, but which may contain intentional typos to trick individuals. For example, a phishing attack may direct someone to a fake website that uses 1's (ones) instead of l's (i.e., a11phishes vs. allphishes).
- Use multi-factor authentication. Multi-factor authentication reduces the possibility that someone can hack into your account using only your password. OCR's November 2016 cybersecurity newsletter included information on types of authentication.[2]
- Keep anti-malware software and system patches up to date. If you do fall for a phishing scam, anti-malware software can help prevent infection by a virus or other malicious software. Also, ensuring patches are up to date reduces the possibility that malicious software could exploit known vulnerabilities of your computer's or mobile device's operating system and applications.
- Back up your data. In the event that malicious software, such as ransomware, does get installed on your computer, you want to make sure you have a current backup of your data. Malicious software that deletes your data or holds it for ransom may not be retrievable. Robust, frequent backups may be the only way to restore data in the event of a successful attack. Also, be sure to test backups by restoring data from time to time to ensure that the backup strategy you have in place is effective.

There are many resources available to help people identify and avoid phishing attacks. For additional information, please visit the resources below.

- Federal Trade Commission (FTC) consumer information on phishing https://www.consumer.ftc.gov/articles/0003-phishing
- Federal Bureau of Investigation (FBI) information on spear phishing https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109
- Department of Homeland Security (DHS) video to protect against phishing attacks https://www.dhs.gov/science-and-technology/cyber-tip-become-cyber-savvyprotect-against-phishing-attacks

[2] https://www.hhs.gov/sites/default/files/november-2016-cyber-newsletter.pdf