

CYBERSECURITY CYBER-ATTACK SERIES

PHISHING

Prepared by Keith J. Gomes, J.D., Ph.D.

What is Phishing?

Phishing refers to the process where a targeted individual is contacted by email or telephone by someone posing as a legitimate institution to lure the individual into providing sensitive information such as banking information, credit card details, and passwords. The personal information is then used to access the individual's account and can result in identity theft and financial loss. Phishing can also refer to the cybercrime where an imitation of the website of a company is created by phishers to cheat users into providing sensitive information.

Types of Phishing Attacks

To prevent Internet phishing, users should be cognizant of and be able to recognize the various types of phishing techniques and they should also be aware of anti-phishing techniques to protect themselves from getting phished. Some of the most common kinds of phishing attacks include the following:

- 1. Deceptive Phishing:** The most common phishing technique is using deceptive email message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams should raise user suspicion as they most likely lead to a malicious link or seek to obtain confidential information.
- 2. Malware-Based Phishing:** This refers to scams that involve running malicious software on users' devices. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities such as those associated with out-of-date software applications.
- 3. Keyloggers and Screenloggers:** These are tyoes of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started as well as into system files as device drivers or screen monitors.
- 4. Session Hijacking:** This describes an attack where users' activities are monitored until they sign in to a target account or transaction and establish their bona fide credentials. At

- *Over half of Internet users get at least 1 phishing email per day.*
- *Over 100 billion spam emails are sent each day (as of 2011).*
- *According to [Consumer Reports](#), the cost of phishing is nearly \$500 million per year in the United States alone (Computer Associates 2007).*

(U.S.) Main Office & Mailing Address: 347 Fifth Avenue, Suite 1402-285. New York, New York, 10016, USA

(U.S.) 2nd Office Location: 326 Broad Street, Utica, New York 13501, USA

(Canada) Mailing Address: PO BOX # 47056. 2638 Innes Road. Ottawa, Ontario. K1B5P9 CANADA

(Canada) Office Address: 255 Centrum Blvd., Suite 102, Ottawa, ON, K1E 3W3 CANADA

T: 646-205-2246 T2: 613-286-6484 URL: www.XAHIVE.com, Email: sem@xahive.com

that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

5. **Web Trojans:** This form of malware pops up invisibly when users are attempting to log in collect the user's credentials locally and transmit them to the phisher.
6. **System Reconfiguration Attacks:** This modifies settings on a user's PC device for malicious purposes. For example, URLs in a favorites file might be modified to redirect users to fake sites.

7. **Data Theft.** Data theft is a widely used method of business espionage. By stealing confidential communications, design documents, legal opinions, employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

"In 2015, large businesses targeted for attack once was most likely to be targeted again at least three more times throughout the year. All businesses of all sizes are potentially vulnerable to targeted attacks. In fact, spear-phishing campaigns targeting employees increased 55 percent in 2015. No business is without risk."
(Symantec 2016)

8. **DNS-Based Phishing ("Pharming"):** Pharming is the term given to hosts file modification or Domain Name System (DNS)-based phishing.

With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that requests for return a bogus address and subsequent communications are directed to a fake site. This may result in users not even being aware that the website where they are entering confidential information is controlled by. Also related to pharming is hosts file poisoning by which hosts files are infected to direct users to phoney websites.

9. **Content-Injection Phishing:** This describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.

10. **Man-in-the-Middle Phishing:** This is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

11. **Search Engine Phishing:** This occurs when phishers create websites with attractive (often too attractive) sounding offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks. Victims who use these sites to save or make more from interest charges are encouraged to

transfer existing accounts and deceived into giving up their details (Computer Associates 2007).

Features of Phishing Emails

Some specific features to watch out for from phishing emails include the following:

- **Luring emails:** Phishing scams often include lucrative offers and eye-catching or attention-grabbing statements in the emails. The email may claim that the user has won a prize, a trip or a grand lottery. To prevent phishing attacks, it is best to avoid these emails and not click on any links or open any attachments.
- **Urgent emails:** Another favorite phishing tactic is to ask you to act fast in order to save on a limited special deal. These emails are best ignored. Sometimes, the email will report that a bank account or other online account will be suspended unless personal details are updated immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, it is best to contact the company directly by telephone.
- **Links to another website and popups:** A link may not be all it appears to be. Fraudsters may perform URL spoofing or IDN spoofing by using scripts or HTML commands to construct fake address bar in place of the original address. In most cases, it is safer to ignore emails asking you to update personal information and directing you to a website. Sometimes the website may open a pop-up window in the foreground with the genuine web page in the background to mislead and confuse the visitor thinking that they are still visiting the legitimate website. Sometimes, a visually similar web address is used to take users to a fraudulent webpage. Unfortunately, sometimes even the digital security system may not resolve the problem of phishing because the owner of a phished website can buy a certificate and change the look of a website to make it resemble the genuine website.
- **Spam Mails:** This common phishing involves sending bulk mails to a great number of users with the hope that at least a few users will fall victim to the malicious emails. Users should avoid reading bulk email and set up adequate spam filters to try and limit spam.
- **Generic Names:** Phishing emails are typically sent in batches and generic names are used to send emails. If the emails do not contain the user name, but instead address the user as “Dear Customer”, it should be regarded with suspicion.

Anti-Phishing Techniques

The following summarises some anti-phishing techniques that users can use:

- **Spam filters:** To protect against spam mails, spam filters should be used. The filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it is spam. Occasionally, however, spam filters may even block emails from legitimate sources, so this is not 100% accurate.
- **Safe browser settings:** The browser settings should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when you try to access the website, the address is blocked or an alert message is shown. The settings of the browser should be appropriate to only allow reliable websites to open up.
- **Change passwords often:** Many websites require users to fill in the login information and password while the user image is displayed. This type of system may be open to security attacks. One way to ensure security is to change passwords on a regular basis. It is also a good idea for websites to use a “captcha” system for added security and to prevent attacks from bots.
- **Report:** Banks and financial organizations use monitoring systems to prevent phishing. However, individuals can report phishing to industry groups where legal actions can be taken against these fraudulent websites. Organizations should provide training to employees to recognize phishing risks.
- **Exercise caution:** Phishing often preys on gullible or naïve users to make mistakes. Remember, if a deal is too good to be true, it probably is. Avoid getting lured into fake deals and if verification is required, always contact the company personally before entering any details online. If there is a link to an email, check the address in the link. Safe websites mostly begins with “https”. If the website from the email does not contain “https”, it could be a phishing email (Phishing.org).
- **Educate yourself:** Learn how to determine if you are being targeted by studying various cases of phishing attempts documented by community projects such as www.419eater.com .



Your Cybersecurity Partner

References

Computer Associates. 2007. "Types of Phishing Attacks." *PC World*. September 12. Accessed July 20, 2016. <http://www.pcworld.com/article/135293/article.html>.

Phishing.org. n.d. "What is Phishing?" *Phishing.org*. Accessed July 13, 2016. <http://www.phishing.org/what-is-phishing/>.

Symantec. 2016. "2016 Internet Security Threat Report." *Symantec*. Accessed July 15, 2016. <https://www.symantec.com/security-center/threat-report>.