TMA Privacy and Civil Liberties Office Information Paper

PHISHING OVERVIEW

Phishing ◆ December 2009

What is Phishing?

Phishing is the fraudulent process of attempting to acquire personal information such as usernames, passwords, credit card details, bank account information, and Social Security Numbers by claiming to be a trustworthy company or organization through an electronic communication. Individuals who engage in this activity, referred to as phishers, typically use e-mails and instant messages that claim to be from a legitimate business or organization in order to play on the credibility of that company to gain access to the sensitive information. As a form of identity theft, phishing can threaten the privacy and security of individuals and entities.

Responding to Phishing:

Concerns about any phishing communications received should be discussed with managers or security officers immediately.

- If a phishing incident is detected, report it to the local Information Assurance Officer or Help Desk. Forward phishing e-mails to spam@tma.osd.mil.
- If a fraudulent link has been opened, contact the local Help Desk immediately.
- If the information released included protected health information (PHI) or personally identifiable information (PII), contact the TMA Privacy Office at privacymail@tma.osd.mil. Provide a brief description of the event, including when it occurred, details of the request, and types of information disclosed.

Additional information on responding to phishing can be found on the Anti-Phishing Working Group's Web site at http://www.antiphishing.org/consumer_recs2.html.

Phishing Techniques:

There are numerous avenues that phishers employ in an attempt to gain access to information, including:

- **Social engineering** – Phishing e-mails and pop-up messages request that an individual update or validate account information and often threaten dire consequences for a lack of response.
- **Link manipulation** – Most methods of phishing use some form of electronic deception to make a link appear to belong to a legitimate organization such as a bank or department store.
- **Filter evasion** – As e-mail spam filters have progressed in preventing fraudulent e-mails from arriving in an individual's inbox, phishers have adapted their methods to circumvent these filters

by using images and photos instead of text.

- **Web site forgery** – Just as links can be manipulated, so can the look of a Web site. This is done by overlaying fraudulent links with a picture of the actual Web site.
- **Phone phishing** – Phishing messages can also provide a phone number for individuals to call in order to verify their information. The phone number provided is usually provided through a Voice over Internet Protocol (VoIP) service and uses fake caller-ID data to give the appearance of a trusted business.
- **Spear phishing** – A more focused attempt, known as spear phishing, uses the same methods to trick a targeted group of individuals into providing information, sometimes on specific information systems, by making the requests appear to come from an individual of authority within the potential victims' organization.

Anti-phishing Techniques:

There are several best practices individuals can employ to protect themselves and their organizations from unwanted attacks and potential harm to their reputation, identity, financial position, and personal security, including:

- Do not reply to an e-mail, text, or pop-up message that asks for personal or financial information, and do not click on links in the message. To go to a bank or business Web site, type the Web address into the browser.
- Do not respond to messages – by e-mail, pop-up, or phone – that request a telephone call to update an account or ask for personal information. To reach an organization, call the number listed on a billing statement or in a phone directory.
- Do not give out personal information without first finding out how that organization intends to use the information and how it will be protected.
- Carefully read Web site privacy policies. They should explain what personal information the Web site collects, how the information is used and whether it is provided or sold to other parties. They should also explain what security measures are taken to protect private information.
- Examine links to see if they appear to be legitimate. Indicators such as misspelled words might suggest that a link to a Web site is fake.

Phishing Resources:

- Anti-Phishing Working Group, What To Do If You've Given Out Your Personal Financial Information, (http://www.antiphishing.org/consumer_recs2.html).
- DISA, Phishing Awareness, April 2008 (http://iase.disa.mil/eta/phishing/Phishing/launchPage.htm).
- FTC, How Not to Get Hooked by a 'Phishing' Scam, October 2006 (http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm).
- MHS Information Assurance Implementation Guide No. 3, Incident Reporting and Response Program, 19 July 2005, (http://www.tricare.mil/tmis_new/ia/3%20-%20Incident%20Reporting%2020090608.pdf).
- OnGuard Online, Phishing, February 2008 (http://www.onguardonline.gov/topics/phishing.aspx).