Risk Solutions

A Business Guide to Preventing, Detecting and Responding to a Phishing Attack

Phishing, pronounced "fishing," is a scam where Internet fraudsters send e-mail spam or pop-up messages (i.e., crimeware) to lure personal and financial information from unsuspecting victims. The e-mail or message directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card information, Social Security numbers, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Recently, fraudsters have increased their phishing activities dramatically. The Anti-Phishing Working Group (APWG), a consortium of Internet service providers, security vendors, financial institutions, and law enforcement agencies, reports that the number of sites infecting PCs with password-stealing crimeware reached an all-time high of 31,173 in December 2008, an 827 percent increase from January 2008

The U.S. Department of the Treasury has worked with businesses that have been victimized to identify measures to prevent, detect, and respond to phishing attacks. These measures are summarized below.

Measures to Prevent Falling Victim to Phishing

- Personalize e-mails to consumers so that they are assured of their legitimacy.
- Keep Web site certificates up to date so that consumers are assured of the site's legitimacy.
- Remind consumers to obtain and use the latest patch for their Web browser and/or operating system software.
- Provide on Web sites a domestic telephone number for consumers to call to verify e-mail requests for information.
- Register domain names that are similar to that of the firm's so that consumers do not confuse them with the legitimate Web site.
- Establish a trademark for the domain name of the firm. Under the Anticybersquatting Consumer Protection Act, a firm may be able to initiate immediate action in federal district court against a suspicious Web site to protect the firm's trademark.

Measures to Detect Phishing Attacks

- Monitor the use of trademarks and key content by suspicious users on the Internet.
- Monitor the Internet for fraudulent variations of the firm's name, trademark, seal, or Web site address.
- Instruct call center employees to identify and notify management of reports of suspicious e-mails.

continued ▶

Measures to Respond to Phishing

- Promptly post a prominent alert describing the incident on the firm's Web site.
- Contact consumers by e-mail or postal mail warning them not to respond to suspicious e-mails. Remind consumers of the firm's official policy of not soliciting sensitive information through e-mails.
- Alert staff and third-party vendors of an attack and ask that they watch out for unusual activity.
- Advise those consumers who have fallen victim to the attack to change their passwords and report the attack to the Federal Trade Commission (FTC) at http://www.ftc.gov/.
- Contact the Internet Service Provider (ISP) hosting the illegitimate Web site and ask that the illegitimate site be shut down. Ask the ISP to disclose the identity of the owner of the illegitimate Web site.
- Contact a law enforcement agency, such as the field offices of the U.S. Secret Service (http://www.secretservice.gov/field_offices.shtml) or the FBI (http://www.fbi.gov/contact/fo/fo.htm) to pursue a subpoena or other appropriate remedy to identify the owner of the illegitimate Web site.
- Forward any phishing e-mail to the FTC at uce@ftc.gov, or file a complaint on the Identity Theft Web site of the FTC (http://www.ftc.gov/bcp/edu/microsites/idtheft//index.html).
- Report the phishing attack to the Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA), at http://www.ic3.gov/default.aspx.

To learn more about Hanover Risk Solutions, visit hanoverrisksolutions.com

AIX Group™ *A member of The Hanover Insurance Group*

AIX, Inc.
www.aixgroup.com

5 Waterside Crossing, Suite 201
Windsor, CT 06095

860.683.4250 Phone
860.683.4453 Fax

171-0914AIX (3/17) LC 10-185H