

ADVISORY NOTE: IS YOUR COMPANY AT RISK?

Phishing Attacks on the Rise – over 50% Increase Year over Year

Network Appliance, Inc. | June 6, 2004

How the Network Appliance™ Internet Access Security (IAS) Solution Can Help Customers Address This Growing Problem

ADVISORY NOTE

A new Gartner Inc. study reports that phishing scams have exploded in number in the past year, a 50% increase over 2003. As many as 30 million people have been subject to phishing attacks, and 1.78 million people may have fallen victim to the online scams, which are used for identity theft. In the study, 3% of survey respondents reported having been drawn into a phishing scam. Gartner estimates that direct losses from identity theft fraud against these phishing attack victims cost U.S. banks and credit card issuers about \$1.2 billion last year. Typically targets have been financial service companies and retailers. Examples of these incidents have included **America On-Line, Bank of America, Bank One, Citibank, Earthlink, Ebay, FleetBoston Financial Corporation, and US Bank.**

This is a serious threat to your company. Recently news reports from the Anti-Phishing Working Group (APWG) reported a 187% increase from March 2004 to April 2004 (over 1,000 unique phishing campaigns). Fortunately, you can advise your company of the extent of the threat and how you can help them address it with content security from Network Appliance and Webwasher.

Phishing (also called “carding”) is the illegal act of sending an e-mail to a user under the false pretense of being a legitimate enterprise such as a financial institution, service provider, or online retailer. It is used in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to what appears to be the Web site of a trusted service provider, where the user is asked to update personal information, such as passwords and credit card, social security, and bank account numbers. The Web site, however, is an imitation set up only to steal the user's information.

How Network Appliance Can Help

A user's common sense is the best defense against phishing (i.e., there is an increasing awareness that you just don't send personal data such as passwords or bank accounts over the Internet). In addition, the entities whose customers are targeted for this fraud are making a concerted effort to notify customers that they will never request information in this manner. However, organizations and individuals need a higher level of proactive protection. This is where we can help.

1. URL blocking of known phishing Web sites

Working with the FBI, FTC, and local law enforcement agencies, IAS collects URLs of known phishing Web sites. These are entered in the “computer crime” category of the

URL database on a regular basis. There are meetings with local police computer crime

departments to exchange knowledge, get feedback, and develop increasing expertise in detecting phishing scams. In addition, customer experiences provide a source of feedback on these scams.

2. Adding these URLs allows for blocking a large percentage of attempts to visit phishing scam sites, helping to protect employees from divulging personal data to criminals.
3. Spam blocking of phishing scam e-mails that are sent en masse

A spam filter blocks phishing scams that are sent en masse or have special characteristics. IAS then adds new phishing scam sites to its database by automatically extracting URLs contained in the mass of spam collected by honeypots (systems designed to attract and "trap" spammers). The URLs are analyzed via automated and manual methods. URLs that appear to be phishing scams are added to the database's "computer crime" category.

Note: There is no guarantee of detection of all phishing scams. Only a forensic analysis by law enforcement can do so.

ADVISORY NOTE

While regular spam filters already add a level of protection, Webwasher's URL filter takes it to the next level by:

1. Looking at special characteristics such as forged URLs in the body of an e-mail, a phony sender, and atypical mailing programs not used by corporations
2. Querying a URL database with known phishing URLs
3. Sending the suspect URLs to Webwasher experts for further manual inspection

The IAS solution is an on-box joint solution between Network Appliance and Webwasher. Contact your local Network Appliance representative for more information.

Related Links

Phishing E-mail Example

To see an example and analysis of a recent phishing scam, visit [http://antiphishing.org/phishing_archive/04-05-04_US_Bank_\(Internet_banking_issue\).html](http://antiphishing.org/phishing_archive/04-05-04_US_Bank_(Internet_banking_issue).html).

For More Information

Federal agencies and antiphishing organizations provide up-to-date information on phishing scams and Internet fraud. Visit the following Web sites to learn more:

- Anti Phishing Working Group: www.antiphishing.org/
- U.S. Secret Service: www.secretservice.gov/alert419.shtml
- Gartner press release on its phishing study: www4.gartner.com/5_about/press_releases/asset_71087_11.jsp
- May 6, 2004, Infoworld article on the Gartner study: www.infoworld.com/article/04/05/06/HNphishing_1.html



Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
www.netapp.com

© 2002 Network Appliance, Inc. All rights reserved. Specifications subject to change without notice. NetApp and the Network Appliance logo are registered trademarks and The evolution of storage are trademarks of Network Appliance, Inc., in the U.S. and other countries. Webwasher is a registered trademark of Cyberguard Company. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.