



Websense Enterprise “Phishing and other Frauds” Web Filtering Category Protects Organizations against Advanced Internet Scams

Websense, Inc. unites with the Anti-Phishing Working Group to protect employees and fight the spread of phishing and email spoofing

SAN DIEGO June 21, 2004 -- Websense, Inc. (NASDAQ: WBSN), the world's leading provider of employee internet management (EIM) solutions, today announced that Websense Enterprise® has further expanded its ability to protect organizations and their employees from today's advanced internet scams and threats such as phishing. Phishing attacks use spoofed e-mails and fraudulent websites that appear to come from trusted institutions, such as ecommerce and financial sites, which are designed to dupe recipients into divulging confidential information. According to the Anti-Phishing Working Group, phishing attacks soared to a record 1,125 unique schemes in April compared with 402 in March.

As hackers continue to discover ways to bypass current email and Spam filters, only a layered approach at the internet and desktop levels to block access to these deceptive phishing tactics is proven effective. The “Phishing and other Frauds” internet content subcategory, available exclusively within the Websense® Security Premium Group™ (PG), provides superior web filtering security by managing employee access to fraudulent websites. This product coupled with Websense Client Policy Manager™ (CPM) protects organizations and employees at both the gateway and desktop.

“Phishing scams are getting more and more sophisticated, preying on employees who will click on the emailed links to access the corrupt sites,” said Brian Burke, research manager of Security Products, IDC. “Websense Enterprise provides a needed layer of protection to employees by automatically categorizing the phishing sites. This powerful protection could save the inquisitive employee who isn't aware that email they just received, even though it looks legit, is a scam to steal their personal information.”

At the internet gateway, URLs that are identified as phishing exploits will be included in the new subcategory, which is updated daily along with the Websense database downloads. When a block policy for the subcategory is implemented by a customer, employees that click on phishing URLs embedded within emails will be blocked from accessing the counterfeit site. Current customers deploying the Websense Security PG will automatically be upgraded to include the new phishing subcategory free-of-charge.

With Websense CPM, organizations gain additional security against internet frauds at the desktop level. Recent email scams have included executable attachments designed to look like official business questionnaires or forms from financial institutions and other organizations that require user authentication. CPM policies enforce the blocking of unauthorized applications from launching on the employee desktop. For example, if an email were to bypass Spam filters and an employee tried to launch a fraudulent application, CPM would recognize this launch request and terminate the application on the desktop before it can cause harm.

“All it takes is one employee to succumb to a phishing scam and all of a sudden confidential business passwords are in the hands of a hacker, putting at risk the intellectual capital of the business,” said Leo J. Cole, vice president of marketing, Websense, Inc. “It's human nature to respond to a request from what appears to be a trusted business institution, even though it is actually a phishing scam. Websense reduces the risks of employees being lured into such scams by automatically blocking access to these dangerous sites. There is no need to second guess on behalf of the employee.”

Websense is taking an active stand to eradicate phishing threats for organizations and their employees around the globe. Websense is the first company in the EIM space to join the Anti-Phishing Working Group (APWG) (www.antiphishing.org), an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. This alliance will benefit Websense customers with advanced warning of advanced phishing threats and will serve as a powerful resource for the Websense URL database. In addition, automated search processes and Websense's honeynet, a series of “honeypots” which attract and “trap” unauthorized attempts to penetrate victim's computer systems, routinely discover new internet frauds. As new scams are discovered, these websites will quickly be added to the database and automatically sent to Websense Security PG customers.

“Phishing attacks continue to increase and pose a significant threat to businesses and consumers,” said Dave Jevans, senior vice president, Tumbleweed Communications and chairman, Anti-Phishing Working Group. “We commend Websense for taking an active role in the war against phishing and we look forward to their participation in the fight against email fraud.”

About the Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is focused on eliminating the problem of phishing and email spoofing attacks, by developing and sharing information about the problem, and promoting the visibility and adoption of industry solutions. Membership in the group is open to qualified financial institutions, corporations, law enforcement agencies, public policy groups and solution vendors.

The website of the Anti-Phishing Working Group is www.antiphishing.org. It serves as a public and industry resource for information about the problem of phishing and email fraud, including identification and promotion of pragmatic technical solutions that can provide immediate protection and benefits against phishing attacks. The analysis, forensics, and archival of phishing attacks to the website are currently powered by Tumbleweed Communications' Message Protection Lab™.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), the world's leading provider of employee internet management solutions, enables organizations to optimize employee use of computing resources and mitigate new threats related to internet use including instant messaging, peer-to-peer,

and spyware. By providing usage policy enforcement at the internet gateway, on the network and at the desktop, Websense Enterprise software enhances productivity and security, optimizes the use of IT resources and mitigates legal liability for our customers. Websense serves more than 21,200 customers worldwide, representing 16.8 million seats. For more information, visit www.websense.com.

MEDIA CONTACT

Cas Purdy
Senior Manager, Public Relations
Websense, Inc.
Phone: 858.320.9493
cpurdy@websense.com

© 2004, Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

© 2008 Websense, Inc. All Rights Reserved.