

# TippingPoint Phishing Protection Solution Brief

IPS-Secured Networks

SOLUTION BRIEF – Phishing

Identity theft through phishing scams has become a major enterprise concern. Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords, credit card details and financial account details by masquerading as a trustworthy entity. Since phishing scams usually appear to come from a trustworthy source, they are extremely difficult to prevent and can be very costly to those who fall prey and potentially dangerous to their employers. The TippingPoint IPS is the most comprehensive, network-based solution, able to block phishing attempts by using a variety of security techniques at every step in a phishing attack campaign.

## Network-Based Phishing Protection

- Vulnerability Filters
- Pattern-Matching Signatures
- Behavior-Based Protection Techniques
- Content Inspection

## Comprehensive Phishing Protection

### Against:

- Initial Web Site Compromises
- Mass Phishing E-mails
- Clickthroughs on Misleading URLs
- Displays of Phish Web Sites
- Submissions of Personal Information

## How Big is the Phishing Problem?

As a successful and lucrative form of financial fraud, phishing made its mark on the network landscape in 2004 and continues to be a booming segment of the identity theft industry.

By July 2007, the phishing problem had reached the following levels<sup>1</sup>:

- Unique phishing reports 23,917
- Unique phishing sites 30,999
- Brands hijacked by phishing campaigns 126
- Cumulative financial losses from phishing \$2.8B<sup>2</sup>
- Percent of phishing e-mail links clicked 24.9%<sup>2</sup>

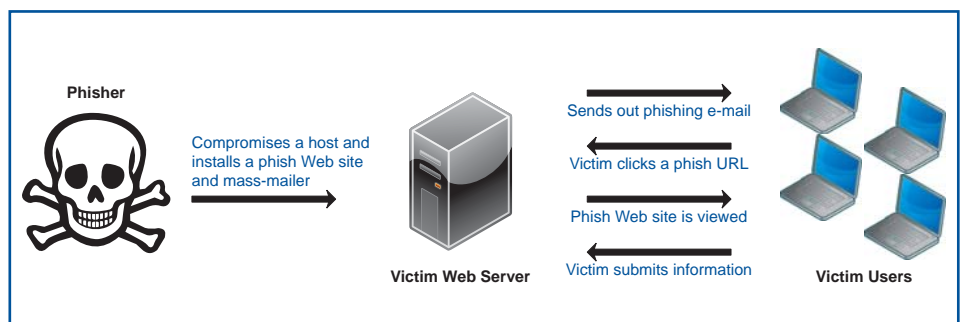
## Obstructing Phishing Attacks

Phishing attacks consist of multiple steps, as shown, that all must occur for an attack to succeed. Fortunately, TippingPoint's Phishing Protection solution can detect and automatically

block the attack at every stage. TippingPoint's Phishing Protection is an extension of the market-leading, award winning TippingPoint Intrusion Prevention System (IPS). With Phishing Protection, the TippingPoint IPS thwarts phishing e-mail scams to protect end users and enterprises from financial losses and protect enterprises from unauthorized phishing operations within their networks or on their Web servers. TippingPoint's IPS, sitting in-line in the network, provides comprehensive protection at the logical transaction phases of a phishing campaign:

### (1) Initial Web Site Compromise

In order to launch a phishing campaign, phishers compromise a legitimate site or server by taking advantage of programming flaws in the Web site code and system flaws in the server. Many solutions are designed to detect and prevent general compromises, but only the TippingPoint IPS has the extended capability to specifically protect against Web site or server compromise attempts.



TippingPoint®

TippingPoint Phishing Protection	Customer Benefit
<u>Blocks</u> initial Web site compromise	<ul style="list-style-type: none"> <li>• <b>Minimize legal and financial risks</b> by preventing the compromise of corporate Web pages</li> <li>• <b>Minimize compromise of enterprise systems</b> such as Web mail, from stolen employees credentials</li> <li>• <b>Reduce network security complexity</b> by automatically preventing phishing attacks with a single IPS solution and single management console</li> <li>• <b>Reduce IT staffing demands</b> since attacks are automatically blocked and no reactive follow-up investigation is required</li> </ul>
<u>Blocks</u> mass phishing e-mails	
Detects fraudulent URLs & <u>blocks</u> Web site load	
Detects Web site forgeries & <u>blocks</u> Web site load	
<u>Blocks</u> private information posting	
Shipped with most filters already enabled in recommended settings	<ul style="list-style-type: none"> <li>• <b>Easy to deploy</b> phishing protection using a IPS solution that requires no initial device configuration</li> </ul>
On-going Digital Vaccine updates	<ul style="list-style-type: none"> <li>• <b>Reduce IT staffing demands</b> as all device updates are automated and require no IT intervention</li> <li>• <b>Automatic protection</b> against evolving phishing tactics</li> </ul>
Network-based solution	<ul style="list-style-type: none"> <li>• <b>Easy to manage</b> phishing protection with no client software to deploy, manage or update</li> </ul>

The TippingPoint IPS offers comprehensive protection against these targeted attacks by blocking the attempted exploit of vulnerabilities, including those in network infrastructure or even Web site code, such as HTML, PHP, ASP and JavaScript vulnerabilities.

## (2) Mass Phishing E-mail

Once a phishing Web site is in place and appears as a legitimate site of a well known financial institution, the next stage of the phishing campaign begins with the phisher uploading his mass-mailer of choice, along with a pre-written HTML e-mail body and address list. The mass mailer is designed to deliver messages at a reasonable speed while at the same time disguising the message from most common spam-detection methods. The TippingPoint IPS analyzes email headers and

content for defining characteristics, using pattern-matching and behavior-based techniques to block phishing e-mails at the mail gateway so that it never reaches the intended recipient.

## (3) Victim Clicks on Misleading URL

The e-mail directs the user to visit a Web site where they are asked to update or insert personal information. This stage of the attack is largely outside the phisher's control. The attack is wholly reliant on the presumed veracity of the crafted e-mail and the users' lack of phishing awareness. Because there is a tendency for phishers to recycle the same campaign over and over again, certain patterns have surfaced in the structure of the victim's first exposure to a given phishing site, which the TippingPoint IPS can easily recognize and block.

## (4) Phish Web Site is Viewed

At this point in the campaign, the victim has been convinced of the phish e-mail's authenticity, has clicked the provided link, and is now loading the phisher's forged Web page. The TippingPoint IPS uses its vulnerability and behavior-based filters to protect the end user. Because several phishing sites take advantage of vulnerabilities in Internet Explorer, Outlook, and other popular Web browsers and e-mail clients, the TippingPoint IPS can determine if the Web site is forged by detecting these vulnerabilities. The TippingPoint IPS also inspects the fraudulent Web page for defining content and common characteristics of many phishing campaigns.

## (5) Victim Submits Account Information

At the final stage of the attack, the victim is poised to submit his information to the phisher, which is usually account information, such as a credit card, banking information, or identification information. TippingPoint's filters for this form of phishing attack prevent the "bad behavior" at the last possible moment and accurately identify the highest risk victims and the IP address of the active phishing site.



<sup>1</sup> "Phishing Activity Trends." July 2007 *Anti-Phishing Working Group*. [http://www.antiphishing.org/reports/apwg\\_report\\_july\\_2007.pdf](http://www.antiphishing.org/reports/apwg_report_july_2007.pdf)

<sup>2</sup> Litan, Avivah. "Phishing Attacks Leapfrog Despite Attempts to Stop Them." *Gartner*. 1 November 2006 <http://www.gartner.com>.

### Corporate Headquarters:

7501B North Capital of Texas Hwy.  
Austin, Texas 78731 USA  
+1 512 681 8000  
+1 888 TRUE IPS

### European Headquarters:

World Trade Centre Amsterdam  
Zuidplein 36, H-Toren  
1077XV Amsterdam  
The Netherlands  
+31 20 799 7629

### Asia Pacific Headquarters:

30, Cecil Street, #18-01  
Prudential Tower  
Singapore 049712  
+65 6213 5999