

Anti-Phishing Solution

Protects Corporate Users and Networks Against Sophisticated Phishing Attacks

Prevent Identity Theft and Safeguard Information Assets

Today's cybercriminals are motivated by financial gain, and their main vector of attack has become the Web. One of the techniques they use is Phishing (pronounced "fishing"), which relates to Web attacks aimed at fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity.

Phishing presents a problem for corporations. If their employees are not protected, enterprises could be held liable for not putting protections in place to prevent fraud. An attack could also result in employee login information being compromised, allowing a cybercriminal to get access to an employee's network account and thus accessing confidential information.

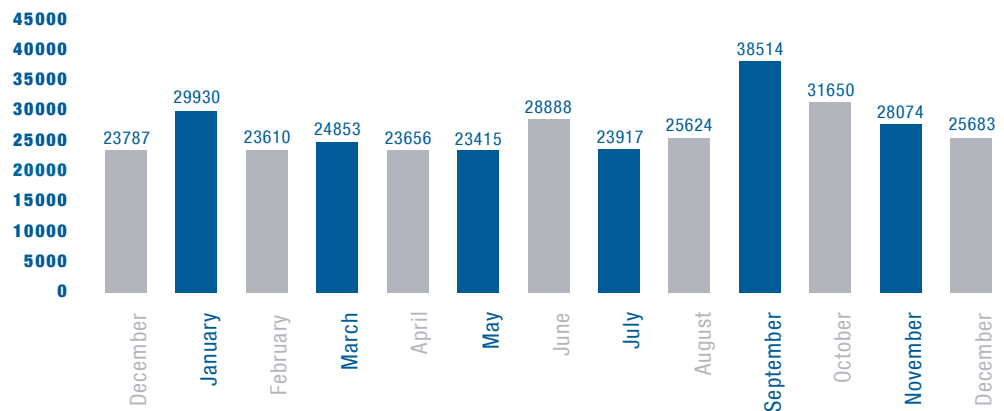
Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering techniques, such as spoofed emails and fraudulent websites, are used to trick recipients into revealing personal data such as credit card numbers, account usernames and passwords and social security numbers.

Phishing attacks lure their targets to a fraudulent site designed to look like one from a legitimate institution, in most cases a bank or e-commerce company.

The Anti-Phishing Working Group noted that in the December 2007 reports from the field, phishing attacks spoofed websites of national tax revenue agencies in the United States, Australia and the UK and, at the same time, previously untargeted segments, such as motorists associations.



Phishing Reports Received December 06 / 07



Phishing Reports Received, December 2006 – December 2007

An integral part of Finjan's Vital Security™ Web Appliances for businesses and organizations, our Anti-Phishing solution provides superior protection against sophisticated Phishing attacks, without compromising your organization's productivity or performance.

This solution uses multiple technologies to prevent Phishing attacks that can result in severe damages to both organizations and individuals.

How Active Real-time Content Inspection Protects against Phishing

Active real-time content inspection protects the networks and vital information assets of organizations around-the-clock. Finjan's Secure Web Gateway products utilize active real-time content inspection to understand the intended criminal behavior of web content. Each and every piece of incoming and outgoing web content, including HTTP/HTTPS content, is analyzed in real time regardless of its originating URL and without signature matching. It therefore detects and blocks Phishing attacks, thus protecting enterprises from any Phishing that may result in severe business damage.

Finjan's Anti-Phishing Solution

Finjan's Anti-Phishing Solution combines Finjan's active real-time content inspection technology with industry-leading URL filtering engines to provide superior protection against phishing attacks. Finjan's Anti-Phishing Solution identifies malicious active content associated in URLs, and blocks it at the gateway. It therefore provides excellent protection against sophisticated phishing attacks.

- Scanning for known hacking techniques used to replace the web browser address bar with a fake one, including malicious JavaScript, and proactively blocking such attempts.
- Leading URL Filtering engine categorizes known Phishing sites and blocks users from accessing.
- If the fraudulent site also contains malicious code (such as Crimeware, Spyware, Trojans and other types of malware), such content is detected and blocked by Finjan's active real-time content inspection technology.
- Finjan's SSL Inspection module protects against phishing attacks that use invalid, revoked or otherwise problematic certificates by enforcing your organization's certificate policies at the gateway.
- Phishing attacks using SSL-encrypted content are also identified and blocked by Finjan's active real-time code inspection.

For Additional Information

For more information, please visit www.finjan.com or contact our regional offices:

USA

Toll Free: 1 888 FINJAN 8 (1 888 346 5268)
Tel: +1 408 452 9700
Email: salesna@finjan.com

United Kingdom

Tel: +44 (0)1252 511118
Email: salesuk@finjan.com

Germany

Tel: +49 (0)89 673 5970
Email: salesce@finjan.com

The Netherlands

Tel: +31 (0)33 454 3555
Email: salesne@finjan.com

Asia Pacific

Tel: +972 (0)9 864 8200
Email: salesapac@finjan.com

Israel

Tel: +972 (0)9 864 8200
Email: salesis@finjan.com

Finjan - Securing Your Web

Finjan Secure Web Gateway Appliances for Enterprises



NG-8100



NG-6100



NG-5100

© Copyright 1996 - 2009. Finjan Inc. and its affiliates and subsidiaries. All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan. The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including European Patent EP 0 965 094 B1 and U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744, 7418731 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dot, Window-of-Vulnerability, RUSafe and SecureBrowsing are trademarks or registered trademarks of Finjan Inc., and/or its affiliates and subsidiaries. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. IBM Proventia Web Filter technology is a registered trademark of IBM Internet Security Systems. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl and Websense are registered trademarks of Websense, Inc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation.

All other trademarks are the trademarks of their respective owners. Q1 2009.