WHITE PAPER: MESSAGING SECURITY

Symantec Brightmail™ Anti Phishing

Confidence in a connected world.

symantec™

White Paper: Messaging Security

Symantec Brightmail™ Anti Phishing

Contents

Introduction

In today's information driven world, cyber criminals are more active than ever before and putting the average computer user and organizations at risk of significant data, brand and financial loss. One method that is frequently employed is phishing, which the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details by appearing as a trustworthy entity in an electronic communication. Examples of phishing include communications to unsuspecting end users purporting to be from financial Institutions, popular social websites, auction sites, online payment processors or IT administrators. Typical channels for phishing are e-mail or instant messaging, and often direct users to enter details at a fake website which made to look and feel like a legitimate one.

Despite the use technology to combat phishing attempts, it normally requires tremendous skill to detect that a website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current Web security technologies. While legislation has been enacted to battle this problem, it shows no signs of slowing down. The Symantec monthly *State of Phishing* report[1] details phishing activity on a monthly basis, keeping both organizations and home computer users informed and helping them avoid becoming victims of phishing attempts.

In addition to implementing technology to help protect against malicious activity on the Web and email, organizations must educate their end-users on phishing to avoid the negative impact of being victimized. Phishing attacks present serious consequences for organizations including loss of data, financial losses as well as loss of brand due to the negative publicity associated with these cases. In today's economic climate, companies can ill afford the loss of brand which ultimately can mean a shrinking customer base.

Symantec, with its collection of people, processes and solutions, is uniquely positioned to win the fight against phishing and other cyber-related criminal activity.

1-Symantec monthly State of Phishing report; www.symantec.com/spam

Intelligence gathering

Recently, there have been cases where a large organizations were the target of phishing attempts. In one such case, users at an organization received emails that came via SMTP, directing them to click on a URL within the email. The ultimate goal of this phishing attempt was to gain access to information, ultimately leading to financial loss for the company. In another case, end users were sent an email via a Webmail application asking them to provide their username and password. The email, shown below, looks the same as any other message associated with accounts that typical computer users have online asking them to update their information, and thus can easily trick end users into providing credentials to a criminal entity. In both cases, implementing the right technology and educating end users would help in allowing organizations to avoid the negative impact of a successful phishing attempt.

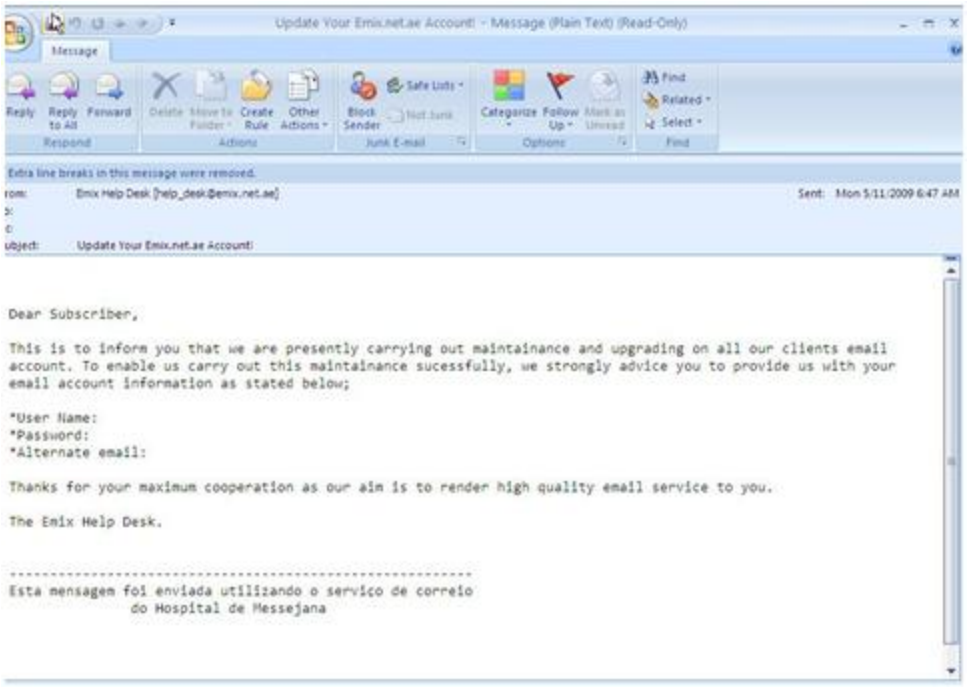

Figure 1. Example of a Phishing email

Symantec leverages multiple sources to gather intelligence and data on phishing, spam, viruses and other types of malware. This data is analyzed and leveraged by Symantec's portfolio of solutions to help customers protect their organizations from threats to their messaging systems, IT infrastructure, and loss of valuable data. At the core of Symantec's backend technologies is the Symantec™ Global Intelligence Network, which encompasses some of the most extensive sources of Internet threat data in the world to offer comprehensive and up-to-date. Elements of the Global Intelligence Network focused on phishing include the Symantec Probe Network: more than two and a half million decoy email accounts focused on collecting fraud, phishing and spam samples.

In addition to focused techniques, the Global Intelligence Network has monitored security devices which log up to 2 billion daily events, helping Symantec understand what threats are impacting our customers. In addition to that, 120 million virus submission systems provide insight into the latest threats, along 40 thousand sensors in over 200 countries which determine where threats originate and whether or not they are targeted or global.

At the heart of this intelligence gathering network is the Symantec Security Response team, which has been combating threats for over 15 years and consists of more than 200 security specialists working around the clock, 365 days a year. Security research centers around the world provide unparalleled analysis of and protection from malware, security risks, and vulnerabilities. In addition to the more than 200 Security Response specialists, Symantec has a global team of intrusion experts, security engineers, virus hunters, threat analysts, and technical support professionals who provide fast and accurate analysis of security data—24 x 7—to help customers guard against complex Internet threats and other security risks.

Conclusion

While there are many technologies on the market that help organizations protect and defend against phishing attacks, none are as deep and extensive as that of Symantec's Brightmail line of products. Other solutions are largely dependent on their own administrators and end-users submitting missed phishing emails in a timely manner to corresponding back-end operations teams, a very manual process. This can also lead to increased administrative overhead and burden on systems. Symantec's Global Intelligence and Probe networks are uniquely positioned to help organizations protect against phishing attacks though automated systems and processes which have deep visibility into all global threats, thus taking the burden off of the end user and ensuring complete protection at all times.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

12/2009 20717027