WHITE PAPER

Symantec Online Fraud Management

Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization

INSIDE

- New online threats
- Impacts on customer trust and brand confidence
- Getting upstream of the problem with blocking and alerting
- Customer education and protection methods
- Comprehensive online fraud mitigation techniques

Contents

Executive Summary

Due to the thousands of unique online fraud attacks that are being perpetrated on the customers of financial institutions and retailers that offer online services, online fraud seriously threatens the brands and reputations of these enterprises, as well as the confidence of online consumers. Using techniques such as brand spoofing and phishing, criminals are routinely convincing unsuspecting online consumers to surrender passwords, account numbers, Social Security numbers, and other personal information. In many cases, this is leading to a rise in the already pressing problem of identity theft. Mitigating the latest online fraud techniques requires a combination of measures, including fraudulent email detection and blocking, consumer education, and desktop computer security assessment and increased protection. Symantec has developed a comprehensive fraud management system that incorporates each of these key elements, while leveraging its top-rated consumer security products and services. Financial institutions and Web retailers now have a means to stop most fraudulent emails from reaching their customers and protecting the consumers who do receive them. This solution can protect their brand and reputation, preserve customer trust in online transactions, reduce fraud and customer support costs, and aid prosecution of offenders.

Email Fraud Explained

Email fraud involves a deliberate attempt by the sender to defraud using email as the contact mechanism. Fraudulent email is becoming a dangerous force, capturing the attention of the media, corporate executives, legislators, and consumers. This burgeoning category ranges from rudimentary scams to more complex attempts to perpetrate online identity theft or misrepresent the brand of established companies.

The most insidious and damaging varieties of email fraud incorporate two related techniques: 1) brand spoofing, and 2) phishing.

BRAND SPOOFING

Brand spoofing occurs when the perpetrator sends out legitimate-looking email that appears to originate from large or recognizable companies. This form of spoofing extends beyond simple email header spoofing – the routine tactic in which spammers disguise headers to appear to originate from familiar addresses, such as those of coworkers, or simply from untraceable addresses. Brand spoofing emails include deceptive content in the body of the message, fraudulently using the spoofed company’s logo and/or using convincing text that seems to be legitimate. By hijacking brands, scammers can attract the attention of customers and potential customers of the company. Some emails are so convincing that even savvy users are unable to discern the difference between brand-spoofing email and legitimate communication from the company.

PHISHING

For perpetrators of fraud, brand spoofing itself is not the goal. The payoff occurs when recipients are fooled into providing personal and financial information. The term for such malicious attempts to collect customer information for the purpose of committing fraud is phishing (pronounced “fishing,” in which criminals fish for financial information from the sea of online consumers using fraudulent emails as bait). In some cases, phishing is accomplished by directing customers to a fraudulent Web site that appears to be a legitimate site. This site includes instructions or forms that allow the scammer to obtain bank accounts, addresses and Social Security numbers – all the data necessary to commit identity theft.

IDENTITY THEFT

Brand spoofing and phishing are relatively new tools in the arsenal of would-be identity thieves, and are likely to exacerbate what was already a pressing problem for many customers of companies in a range of industries, including financial services. The Identity Theft Resource Center (ITRC) reports that among consumers contacting the Federal Trade Commission (FTC), identity theft is the number one concern. Two studies completed in June 2003 by Gartner Research and Harris Interactive found that approximately 7 million people were victims of identity theft in the previous 12 month period – a significant increase from the previous year. The aftermath of identity theft includes an average of 600 hours per victim to recover from the crime, at a huge cost in lost potential income. Moreover, a 2003 ITRC report concluded that business losses range from $40,000 - $92,000 per name in fraudulent charges[1].

The Growing Threat of Email Fraud

According to the Anti-Phishing Working Group (APWG) – an industry association dedicated to eliminating fraud and identity theft via phishing and spoofing – the number of unique phishing attacks has risen dramatically. Attacks monitored by APWG rose from 116 in December 2003 to 1,422 in June 2004 – a 12-fold increase in this six-month period. Customers of companies in the financial sector (led by attacks on Citibank and U.S. Bank) and the online retail sector (led by attacks on eBay and Paypal) are most often attacked. Citibank customers alone were the target of 492 separate attacks in June 2004, and 1,544 attacks from December 2003 to June 2004. These types of entities in the U.S., the U.K., and Australia appear to be the most targeted[2].

Websense, Inc. contributed various other statistics to the APWG report, including the following:

- Phishing Web sites are not overly concentrated in one country. The U.S. was the country that hosted the most phishing Web sites, with 27 percent of the total, followed by Korea with 20 percent, and China with 16 percent.
- Phishing Web sites have short lives, with an average lifespan of 2.25 days.
- About one quarter of phishing Web sites are hosted on hacked Web servers.
- Almost all phishing Web sites (94 percent) enable their developers to remotely download captured personal data[3].

A Typical Example of Online Fraud

Figure 1 illustrates how the one-two punch of brand-spoofing and phishing can threaten the brand equity of an organization, in this case a fictitious bank. In the latter stages of the fraud, the trust and confidence of customers is undermined.

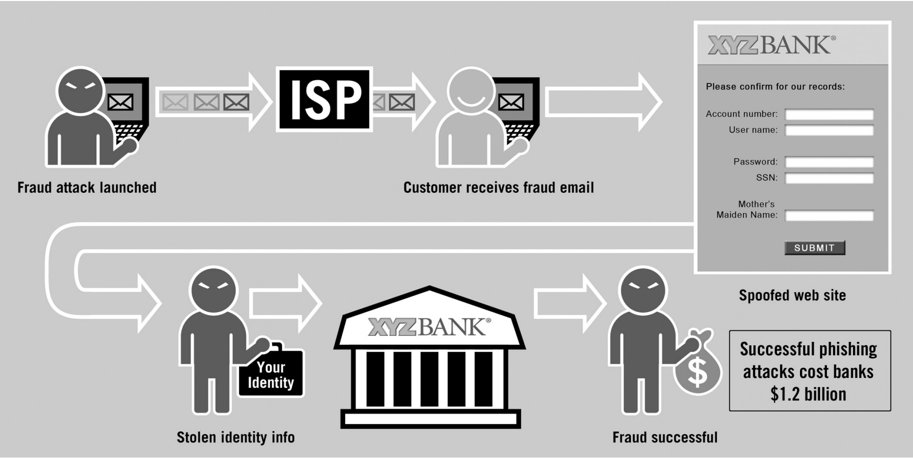


Figure 1. The process of email fraud includes customer receipt of an initial brand-spoofing email, content in the email that lures unsuspecting customers to a Web site that appears to be a legitimate financial institution site, and a request for customer information in an online form.

The Scope of the Threat

Customer trust forms the foundation of the financial services industry. Without this fundamental underpinning, the entire financial services model breaks down. Customers must be able to trust their financial institutions to protect their privacy, and ensure the accuracy of transactions. Phishing attacks threaten this consumer confidence by undermining their trust in online transactions. As a result, many industry observers view phishing as no less than a primary threat to the future of online banking.

In addition to this general threat that the financial services industry faces, individual entities in this industry are now being exposed to potential adverse impacts on their particular brands. Even though phishing scams are perpetrated by parties unconnected with financial institutions, surveys have shown that customers blame their financial institution when their passwords or identity fall into the wrong hands. Depending on the scale of the phishing attack, this “guilt by association” can tarnish the reputation of, the brand loyalty to, and consumer confidence in the bank or other institution.

The financial costs of this form of fraud include direct losses that financial institutions must absorb, which Gartner estimates totaled $1.2 billion in 2003[4]. A second form of financial costs – higher customer service and support costs – rise as a result of the flood of services center calls received from customers who are trying to verify the legitimacy of emails they have received or recover from theft of their identity. Such inquiries can lead to unanticipated spikes in these calls.

Effective Methods of Mitigating Online Fraud

To date, no complete solution that mitigates online fraud has been available. Symantec is working with several industry groups, including APWG and the Financial Services Technology Consortium – Counter Phishing Initiative, to develop technologies that will address this problem in both the short-term and long-term. In the meantime, the FTC and other organizations advocate consumer education on the risks of online fraud, and legal measures can be pursued if the perpetrators of the crime can be identified.

Symantec now offers a multi-pronged technology-based solution for online fraud management. This approach – called the Symantec Online Fraud Management Solution– includes the following components that work together to form a complete solution:

- An email fraud detection, filtering, and alerting network
- On-line customer education
- A desktop security assessment capability for customers of financial institutions
- An infrastructure and means for financial services customers to acquire the products and services needed to improve their level of protection.
- Consulting and assessment services.

The fraud detection network detects and blocks fraudulent email before it reaches financial services customers. In parallel, a single online destination – co-branded with the financial institution – allows customers to better understand security-related and fraud avoidance issues, test their exposure to online threats, and identify and address their security needs.

The Symantec Online Fraud Management Solution enables financial institutions and online retailers to protect their brand and reputation, preserve customer trust in online transactions, and reduce fraud-related customer support and service costs. It also provides a mechanism for gathering information on email fraud perpetrators that ultimately aids prosecution of offenders and protection of legal rights to brand, trademarks, and other intellectual property.

BLOCKING AND ALERTING

A key component of the Symantec Online Fraud Management Solution involves intercepting fraudulent email before it reaches the mailbox of potential victims. Using this approach, damage and costs can be minimized. Figure 2 shows where this aspect of the system operates in the continuum of fraudulent email propagation. The “SMTP phase” is the portion of the process in which the fraudulent emails are disseminated to customers. In the subsequent “Web phase,” customers visit the spoofed Web site, and in some cases, provide personal data in some form. Later in the “offline phase,” customers contact service and support centers. As shown in the illustration, brand and reputation damage increases, and customer confidence erodes, as the process moves

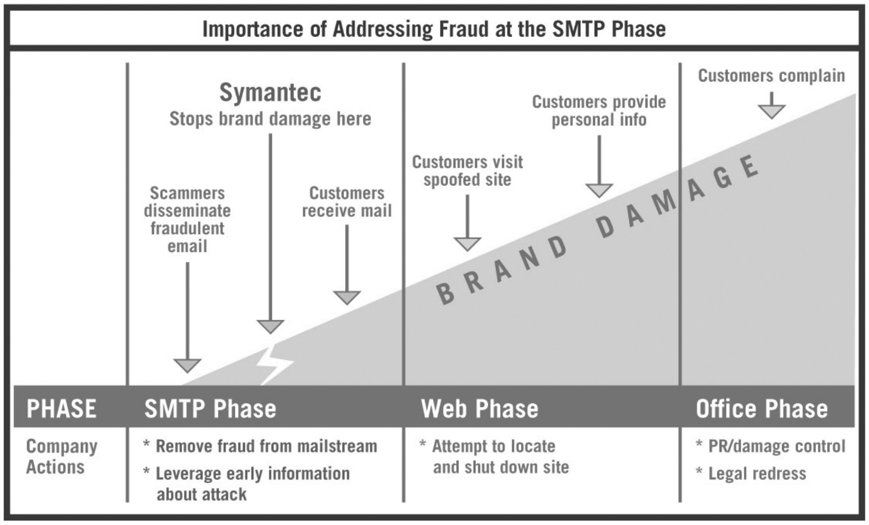

Importance of Addressing Fraud at the SMTP Phase
Symantec
Stops brand damage here
Scammers disseminate fraudulent email
Customers receive mail
Customers visit spoofed site
Customers provide personal info
Customers complain
BRAND DAMAGE
PHASE
SMTP Phase
Web Phase
Office Phase
Company Actions
* Remove fraud from mailstream
* Leverage early information about attack
* Attempt to locate and shut down site
* PR/damage control
* Legal redress

Figure 2. Intercepting fraudulent email before it reaches customers is a key component in an overall strategy to mitigate this threat.

In this part of the Symantec Online Fraud Management Solution, a probe network of two million decoy email accounts attracts fraudulent email. The network then monitors the Internet for fraudulent email that targets the customers of businesses enrolled in this service. At a Symantec operations center, 25 million email messages per day are received and analyzed. Symantec researchers at the center research and validate possible fraudulent email attacks. Unlike spam, fraud attacks can be difficult to detect without expert inspection and detection algorithms. Symantec uses both human experts and technological means to identify fraud attacks at their earliest stages.

Once the fraud attack is identified, Symantec deploys anti-fraud rules in the form of continually updated anti-fraud filters that block fraudulent messages from reaching more that 300 million consumers, thus protecting the majority of the customers of enrolled financial institutions. When attacks that target specific brands are detected, immediate alerts are sent to pre-designated personnel (e.g., the IT administrator on call for the particular financial institution), enabling the financial institution to set in motion incident response procedures such as contacting law enforcement, working to block spoofed IP addresses (see Figure 3), notifying customers, and initiating internal investigations.

The result is that potentially fraudulent emails are automatically filtered and blocked while financial institutions receive immediate notification. Today, Symantec's solution can provide protection for over 300 million email users.

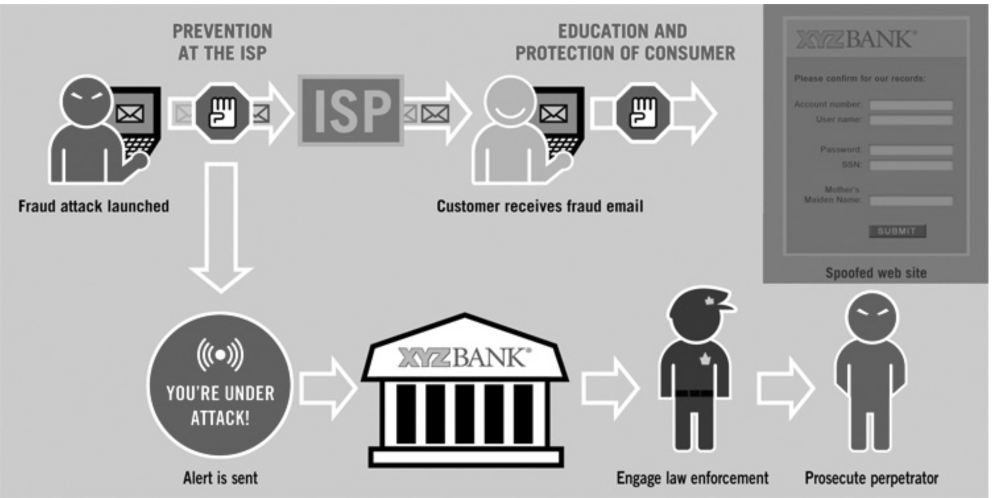


Figure 3. Symantec's Online Fraud Management Solution incorporates fraudulent email blocking, fraud attack alerting, customer education, assessment, and desktop protection combined to prevent online fraud and identity theft.

ONLINE CUSTOMER EDUCATION

Ongoing customer education is central to helping consumers change their behavior to prevent online fraud. Alerting customers of the latest security threats and providing information on how to protect against them is the first step.

Symantec's solution provides information on these and related topics via the Symantec™ Security Connection. From a page on the financial institution's Web site, customers are routed to the Symantec Security Connection, which can be co-branded with the financial institution. This all-in-one, Web-based resource center includes educational articles, expert advice, and real-time security alerts (see Figure 4). This center can help the customers of financial institutions better understand security-related issues.

DESKTOP SECURITY ASSESSMENT

From the same Symantec Security Connection, customers of financial institutions can identify the weak points in their desktop security by performing an online security assessment. A free Web-based tool scans the customer's desktop computer to determine the level of vulnerability and suggests possible solutions to identified vulnerabilities. This tool checks for the following:

- Hacker exposure
- Windows vulnerability
- Trojan horse
- Antivirus product
- Virus protection update

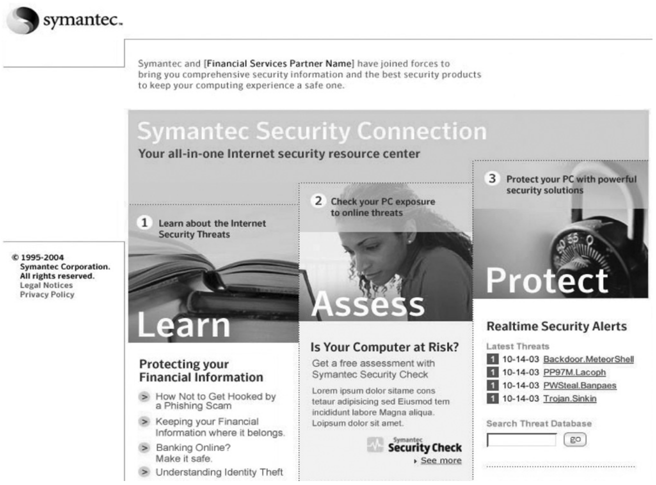
As of November 2003, more than 65 million customers had utilized this service to test the vulnerability of their PC to threats and to learn how to enhance their security.

CUSTOMER PROTECTION

The Symantec Security Connection also enables customers of financial institutions to enhance their protection against email fraud attacks and other security threats via purchase and/or download of products or services identified in the assessment phase.

Symantec provides a number of ways to offer customers additional online protection:

- Discounted software
- Free trial downloads
- Free software (pre-purchased by the financial institution on behalf of its customers).



Symantec and [**Financial Services Partner Name**] have joined forces to bring you comprehensive security information and the best security products to keep your computing experience a safe one.

Symantec Security Connection

Your all-in-one Internet security resource center

© 1995-2004 Symantec Corporation. All rights reserved.
Legal Notices
Privacy Policy

1 Learn about the Internet Security Threats

Protecting your Financial Information

- How Not to Get Hooked by a Phishing Scam
- Keeping your Financial Information where it belongs.
- Banking Online? Make it safe.
- Understanding Identity Theft

2 Check your PC exposure to online threats

Is Your Computer at Risk?

Get a free assessment with Symantec Security Check

Lorem ipsum dolor sitame cons tetaur adipisicing sed Eiusmod tem incididunt labore Magna aliqua. Loipsum dolor sit amet.

3 Protect your PC with powerful security solutions

Realtime Security Alerts

Latest Threats

1	10-14-03	Backdoor.MeteorShell
1	10-14-03	PP97M.Lacoph
1	10-14-03	PWSteal.Banpaes
1	10-14-03	Trojan.Sinkin

Search Threat Database

Figure 4. The Symantec Security Connection provides a one-stop center for customers of financial institutions to learn about fraud-related issues and preventative measures, assess the security of their desktop computer, and enhance their security protection.

A key advantage of this aspect of the Symantec Online Fraud Management Solution is that customers are able to purchase and implement top-rated Symantec consumer products and services from the largest security software company in the world. For example, three Symantec consumer security products – Norton Internet Security™ 2004, Norton AntiVirus™ 2004, and Norton™ Personal Firewall 2004 – earned perfect five-star ratings and were named PC Magazine Editor's Choice award winners in November of 2003. Three months later, a fourth Symantec consumer product – Norton AntiSpam™ 2004 – was also named Editors' Choice by the same journal.

Consulting and Assessment Services

Effective security solutions include an optimal combination of people, processes, and technology. Symantec consulting services in the online fraud area apply this approach, while recognizing that online fraud, including phishing, poses different ramifications for each client organization. Through interviews and research, Symantec Consulting Services assesses a client's:

- Exposure to online fraud
- Planning for handling online fraud, including relevant policies and risk tolerance level
- Compliance with established policy and use of established procedures
- Technology and process controls established to prevent online fraud
- Procedures for identification and prioritization of online fraud incidents
- Procedures for containment and/or eradication of online fraud incidents
- Procedures for follow up and process improvement.

Based on the results and Symantec's best practices, Symantec outlines the client's risks associated with online fraud and delivers detailed recommendations to improve the client's ability to identify, prioritize, and respond to incidents of online fraud.

Benefits of Online Fraud Management Solution

Symantec's Online Fraud Management Solution provides tools to reduce initial exposure to online fraud threats and offers an online resource center that can be co-branded with the financial institution to build brand loyalty and promote trust in online transactions. Benefits to the participating financial institution include the following:

- Protects customers from becoming victims of online fraud
- Protects brand and reputation
- Preserves customer trust
- Reduces support costs from customer inquiries and complaints
- Raises awareness of misuse of brand, trademarks, and intellectual property (IP)
- Protects legal rights to brand, trademarks, and IP
- Enables preventative action against offenders and prosecutorial evidence collection.

References

[1] Identity Theft Resource Center, Facts & Statistics, *http://www.idtheftcenter.org/facts.shtml*.

[2] "Phishing Attack Trends Report, June 2004," Anti-Phishing Working Group, *http://www.antiphishing. org/APWG_Phishing_Attack_Report-Jun2004.pdf*.

[3] "Analysis from Websense, Inc. Incorporated in the Anti-Phishing Working Group's 'Phishing Attack Trends Report,'" August 3, 2004, press release, *http://www.websense.com/company/news/pr/Display.php?Release=040803676*.

[4] "Phishing Attack Victims Likely Targets for Identity Theft," Gartner FirstTake, 4 May 2004, FT-22-8873, Avivah Litan.

For more information on the Symantec Online Fraud Management Solutions visit:
http://ses.symantec.com/onlinefraud

SYMANTEC IS THE GLOBAL LEADER IN INFORMATION SECURITY PROVIDING A BROAD RANGE OF SOFTWARE, APPLIANCES AND SERVICES DESIGNED TO HELP INDIVIDUALS, SMALL AND MID-SIZED BUSINESSES, AND LARGE ENTERPRISES SECURE AND MANAGE THEIR IT INFRASTRUCTURE. SYMANTEC'S NORTON BRAND OF PRODUCTS IS THE WORLDWIDE LEADER IN CONSUMER SECURITY AND PROBLEM-SOLVING SOLUTIONS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS OPERATIONS IN MORE THAN 35 COUNTRIES. MORE INFORMATION IS AVAILABLE AT HTTP://WWW.SYMANTEC.COM.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408 517 8000
800 721 3934

www.symantec.com

For Product Information
In the U.S., call toll-free
800 745 6054

Symantec has worldwide
operations in 35 countries.
For specific country offices
and contact numbers,
please visit our Web site.