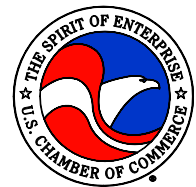


Protecting Your Business and Brand from Online Threats

Prescriptive advice to help protect brands,
infrastructure, and consumers

White Paper
January 2008



Microsoft®

Acknowledgments

This paper reflects input from many organizations and individuals committed to stemming the tide of the deceptive and criminal activities that threaten to undermine customer trust, online confidence, and e-commerce.

Building on the collective experience of Microsoft Corporation and the U.S. Chamber of Commerce and its members, this paper presents best practices and general recommendations for businesses of all sizes. Although there is no absolute defense or guarantee of safety against online threats, businesses that follow these recommendations will be better positioned to reduce online threats and obtain a competitive advantage.

Microsoft would like to acknowledge the support and contributions from the Anti-Phishing Working Group (APWG), Authentication and Online Trust Alliance (AOTA), CA/Browser Forum, Direct Marketing Association (DMA), TRUSTe, and the U.S. Department of the Treasury. The authors would also like to thank Laura Mather - MarkMonitor, Rod Rasmussen - Internet Identity, Michael Chadwick - GoDaddy.com, Aaron Kornblum - Microsoft, and Michael Zanies from the Interactive Advertising Bureau, for their valuable insights and perspectives.

Craig Spiegle
Director,
Windows Internet Security
Microsoft Corporation

Christian Merida
Director,
Congressional & Public Affairs
U.S. Chamber of Commerce

The information contained in this document represents the current view of Microsoft Corp. and the U.S. Chamber of Commerce on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft and the U.S. Chamber of Commerce cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT AND THE U.S. CHAMBER OF COMMERCE MAKE NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Microsoft grants you the right to reproduce this white paper, in whole or in part, specifically and solely for the purpose of personal education.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Microsoft, BitLocker, Forefront, Hotmail, Internet Explorer, MSN, OneCare, Outlook, Windows, Windows Live, and Xbox 360 are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

© 2008 Microsoft Corp. All rights reserved.

Contents

Introduction	1
Value of Domains: Evolution of Infringement	2
Domain Squatters.....	2
Drop-Catching	3
Domain Kiting	4
Domain Spoofing and E-Mail Forgery	4
Targeted Attacks: Spear Phishing and Whaling	6
Fooling Phishing Detectors	7
Proactive Defense Strategies to Thwart Domain Infringement	8
Survey the Internet, Identify Risks, and Monitor	9
Identify Risks.....	9
Proactively Monitor for Phishing Sites	9
Improving Security Infrastructure	10
E-Mail Filtering, Authentication, and Sender ID	12
Harden External-Facing Servers.....	13
Secure and Protect Computers.....	14
Use the Microsoft Phishing Filter	15
Enhancing Trust: Extended Validation SSL Certificates.....	15
Engage with Data Reputation Vendors.....	16
Case Study: The Microsoft Experience	18
Identifying Problem Domain Names.....	18
Securing the Domains.....	19
Proactively Monitoring Domain Names and Web Sites	20
Observing Dangerous Trends	20
Proactively Seeking Spoofed Sites	21
ROI: Phishing Exploits Decrease by 80 Percent.....	21
What to Do If Compromised	22
Creating an Incident Response and Disaster Plan	22
Responding to Incidents.....	23
Conclusion	25
References	26

Situation

Phishing poses a significant threat for individual users and organizations. For individuals, phishing can turn into identity theft; for an organization, phishing sites can compromise brand and company image, as well as the organization's ability to keep the confidence of its customers doing business over the Internet.

Solutions

- Organizations can protect employees and customers by procuring all brand-related and look-alike domain names.
- Businesses can contract with data reputation vendors to publish the addresses of identified phishing sites, helping tools such as the Microsoft® Phishing Filter to warn users who might be drawn to those sites under false pretenses.
- By deploying the Sender ID Framework, organizations can protect their e-mail and domains from forging and spoofing.
- Users can become better educated about how phishers lure victims into their schemes.

Benefits

- Less risk that an organization will be compromised
- Enhanced data governance
- Greater confidence that communication from an organization is legitimate
- Increased deliverability and reliability of legitimate e-mail
- A competitive advantage

Products and Technologies

- Windows® Internet Explorer® 7
- Microsoft Phishing Filter
- Sender ID Framework
- Extended Validation (EV) Secure Sockets Layer (SSL) Certificate
- Windows® BitLocker™ Drive Encryption

Introduction

First published in April 2006, this report has been updated to reflect threats, solutions and recommendations. Although there is no “silver bullet” to protect a business or its infrastructure, a combination of technologies and best practices are required to protect, detect, and remediate online threats. Organizations that adopt the best practices outlined in this paper will become a hardened target, reducing risks and creating a competitive advantage.

The Internet and e-mail have become a vital platform for communication, productivity, and commerce. The combination of Really Simple Syndication (RSS) feeds, instant messaging, e-mail, and the Web has created new markets and opportunities for businesses of all sizes. Unfortunately, the criminal element and unscrupulous businesses are exploiting these avenues and seeking to monopolize these growing opportunities and technologies by stealing personally identifiable information and corporate data.

Thieves and organized crime are systematically pilfering sensitive personal and business data at alarming rates. A study released in December 2007 by Gartner Research estimated 3.6 million adults lost \$3.2 billion as a result of online identity theft, an increase of 1.3 million adults over the prior year. According to USA Today, more than 162 million records were reported lost or stolen in 2007, triple the 49.7 million that went missing in 2006.¹

Although only a small percentage of identity theft has been attributed to online exploits, perceptions are somewhat the opposite as an increasing number of data and privacy breaches are attributed to lost laptops, drives, and mobile devices.

Businesses need to protect themselves and work to improve customer confidence in e-mail and the Internet as a safe way to do business. By working together, sharing best practices and prescriptive advice, collaborating with others in their industry, partnering with law enforcement, and implementing innovative technologies, businesses can better manage the problem.

This paper provides an insider's view of how Microsoft Corporation, a large domain holder, approaches these threats. Incorporating insights from the U.S. Chamber of Commerce and other stakeholders, this paper provides a 360 degree view of recommendations for businesses and organizations of all sizes.

Recognizing that there are other security and safety threats beyond the scope of this paper, the paper focuses primarily on threats that specifically affect a business's brand and customers through deceptive e-mail, phishing exploits, malicious Web sites and fraudulent SSL certificates, and unscrupulous domain registration practices, including domain squatting and drop-catching.

¹ USA Today, Dec. 11, 2007

Value of Domains: Evolution of Infringement

Over the past two years the value of domains has escalated, fostered by live auctions, manipulation, and speculation by buyers and sellers alike. According to the DomainNameNews in 2007, Sex.com sold for a reported \$12 million to \$14 million, topping the charts. DNJournal (<http://dnjournal.com>) reported every domain in the top 100 sold for in excess of six figures.² Legitimate businesses, investors, and others who hope to make a quick buck and resell the domains are aggressively searching out valuable names and domains through a broad range of legitimate and questionable tactics. The rights and assets of brand owners have been under increasing threats, underscoring the need to protect your brand and ensure that your domain does not unwittingly fall into the hands of a third party.

In the late 1990s, Microsoft and many high-value brands first began to experience a variety of online challenges to their brands and trademarks. Web sites began to appear with well-known Microsoft trademarks as well as look-alike and domain names. These sites spoofed Microsoft and deceived customers by attempting to market and sell gray market and counterfeit products; some published deceptive information about Microsoft, its products, its directions, and its intents. Each ultimately compromised the Microsoft image, brands, and reputation—to say nothing of the revenues lost to fraudulent software sales. Over the past decade the industry has witnessed the intent shifting from ad-hoc hackers to malicious threats orchestrated by international crime syndicates, affecting users and businesses worldwide. The following provides an overview of the trends, tactics, and countermeasures a business can employ.

Domain Squatters

Investigation revealed that hundreds of look-alike domain names were registered by what are now referred to as *domain squatters*, *typo-squatters*, or *cyber squatters*—individuals and businesses who have registered domain names with the goal of “ransoming” them to the brand owner, or collecting advertising revenue when users mistype the legitimate URL and click links on those pages. These squatters acquired these names on speculation for a few dollars anticipating that Microsoft (or other corporations) would purchase them at a greatly inflated price. An example of a look-alike domain is www.micrsoft.com, in which “microsoft” is misspelled due to a typing error; the user omitted an “o” between the “r” and the “s.” Legislation has been passed in the United States and elsewhere to help challenge such registrations, and remedies have been established by the Internet Corporation for Assigned Names and Numbers (ICANN), www.icann.org. The courts and ICANN often side with trademark owners, but the legal costs and time for some domains can easily outweigh the cost of just buying the domain name, which works in the domain squatter’s favor.

² www.domainnamenews.com and www.dnjournal.com 1/9/08.

It has been estimated by VeriSign that more than 500,000 domains have been registered solely for extortion from companies that want to protect their brands and trade names. A similar study performed by MarkMonitor (<http://www.markmonitor.com>) revealed more than 382,000 instances of domains being used for domain squatting.

Although this is less than 1 percent of all of the domains registered worldwide, the practice has created a secondary industry in domain names that affects business of all sizes, from home businesses and professional service providers to multinational corporations, financial institutions, and e-commerce sites

To help protect against these squatters, brand owners may want to consider trademark and trade name searches to see if such marks are being used or sold through auctions and brokers. Depending on the legal jurisdiction, the company may contest the domain through ICANN processes and or legal actions to recover the names. As companies and brand owners have successfully increased defenses from this exploit, the cyber squatters have evolved, targeting existing high-traffic domains that expire by using a tactic known as drop-catching.

Drop-Catching

Another entrepreneurial activity has evolved: monitoring the expiration or cancellation of domain names. This trend has been fueled in part by the limited number of words and terms that are left unregistered, names that have been abandoned, and the thousands of domains that expire inadvertently each day. Often the original owner may have changed e-mail addresses or left the company without notifying their registrar, causing them to miss their renewal notices. Known as *drop-catchers*, these “businesses” often acquire a domain name within minutes of a business missing a registration renewal date. The domain is then put up for sale to the highest bidder. This forces the original domain name holder into a bidding war for what it had long thought of as its own property. Drop-catching has even expanded to some domain registrars themselves, who auction the names to the highest bidder in the final days before expiration in the hope that the original owner does not renew.

Even though a company may have gone out of business or a product discontinued, the domain may still have significant value as a result of the existing Web traffic, ad placement, and value to other companies and competitors. According to DNJournal, many such domains have been resold for upwards of \$1 million.

To protect from these risks, businesses should have a centralized management and tracking of all domains being held, including those inactive or acquired for defensive purposes. Centralizing these along with consolidating to a single registrar can yield costs savings and ease of management.

Domain Kiting

Domain kiting exploits an ICANN regulation that allows a domain owner to return a domain within five days for a full refund. Although not the intent of this provision, it allows the purchaser to take five days to determine whether or not the domain will generate enough revenue to justify paying the annual fee. (This is known as *domain tasting*.)

In the domain kiting scheme, the domain owner returns the domain to the registrar within the five day grace period and then immediately reregisters it. Using this technique, the domain owner never pays the registration fee, but continues to use it to generate revenue through pay-per-click advertising.

How does this generate revenue? People or companies who take advantage of the timing of the domain name system buy thousands—even hundreds of thousands—of domains at a time. They put up micro pay-per-click sites heavy with embedded links. When people stumble upon these sites (because, for example, they misspell the name of a popular site) and click the links, the site owner cashes in on the click-through fees.

A recent MarkMonitor study showed that domain kiting represents large percentages of the domains registered in association with brand names. This study reviewed a major U.S.-based financial institution, evaluating all of the domains registered that contained their name, finding more than 1,000 related domains. They found 21.5 percent of the domains hosted pay-per-click pages, taking advantage of domain kiting. The largest percent of the domains (70 percent) appeared to have been abandoned by the original owner, no longer having any company content on the respective Web pages. Such sites indicate they were highly vulnerable to domain kiting.

Domain Spoofing and E-Mail Forgery

Today's e-mail protocol was created more than 25 years ago. It was originally designed to be interoperable and easy to use. Unfortunately, this same functionality has been exploited by spammers and online criminals who forge the "from address" that is visible to a user, purporting to have sent the e-mail from a legitimate company or brand. Such exploits put the user and brand owner at great risk. Users are often directed to deceptive Web sites, which attempt to infect their machine with viruses, keystroke loggers, and malicious software code, as well as subjecting users to the more common tactic of "phishing" personal information and sign-in credentials. Since the "from address" corresponds to a trusted brand, the user is more likely to trust the e-mail message, open it, and click to the deceptive Web site, thereby risking becoming a victim of online fraud. An analysis of inbound e-mail to Windows Live™ Hotmail® in early January 2008 revealed that 10 to 80 percent of e-mail that was purported to come from major brands, ISPs, and banks was spoofed.

Some of the most common forged brands and domains include Yahoo, Bank of America, Verizon, IRS, Comcast, Hotmail, and eBay.³

Addressing this design “flaw” of Internet e-mail, an industry effort has developed several e-mail authentication protocols. A leading solution deployed by more than 15 million domain and brand owners is the Sender ID Framework (www.microsoft.com/senderid). Combined with DomainKeys Identified Mail, (DKIM), a complementary technology, more than 50 percent of all legitimate e-mail sent worldwide daily is now authenticated.⁴ The results have aided in domain and brand protections, while also enhancing the deliverability of legitimate e-mail.

The Phishing Phenomenon

In late 2003, the threat known as phishing (pronounced “fishing”) began to explode across the Internet. Phishing involves tricking unsuspecting users into divulging sensitive personal information such as Social Security numbers, credit card numbers, and Web site passwords.

Phishing began with spoofed or forged e-mail messages that tried to trick recipients into going to a Web site and divulging personally identifiable information. A user receives an e-mail message from what appears to be a legitimate business, usually a well-known brand name and Web site. For example, the fraudulent message might inform the recipient that the company has evidence that someone has been trying to tamper with his or her bank account, and regulations now required the user to sign in to the Web site to change his or her password. Other common examples include sending users an e-mail message asking them to sign in to their account for their monthly statement or to redeem an incentive for updating their account information. By clicking on a link or URL within the e-mail message, the user lands on a Web site that appears identical to the bank’s legitimate Web site. The user is then prompted to enter his or her user name and old password, and to enter a new password. Under the premise of identifying the customer, the site might ask the user to enter other privacy-related questions, such as mother’s maiden name or place of birth. After the user submits the information, the bogus site presents an official-looking page that confirms acceptance of the new password and assures the user that everything will be fine.

But, of course, it is not fine. The trusting user had just given away access to his or her online account. All the work to create a new password was just empty keystrokes—and before the user realizes what has happened, the criminals have compromised, and potentially emptied, the user’s bank account.

The Anti-Phishing Working Group (APWG) reports that the number of phishing sites and phishing e-mail messages continues to climb, to more than 24,000

³ Windows Live Hotmail report 12/2007

⁴ Source: AOTA Jan 2008 State of Authentication Report

unique phishing sites in November 2007. This growing threat is no longer limited to Fortune 500 Web sites. It has migrated to nearly every size of business across all business segments and vertical markets (see Figure 1).

In addition, an increasing number of sites now embed malicious software (or malware), often referred to as spyware or keystroke loggers, on a user's computer. This could put a user's computer at risk just because the user visited the site. The malware's sole intention is to capture confidential personal and business information.

These blended threats also include scripting code that turns an unprotected personal computer into what is known as a "zombie" computer, which can be controlled and monitored by a third party without the user's knowledge—so the threat is even greater than the numbers alone suggest.

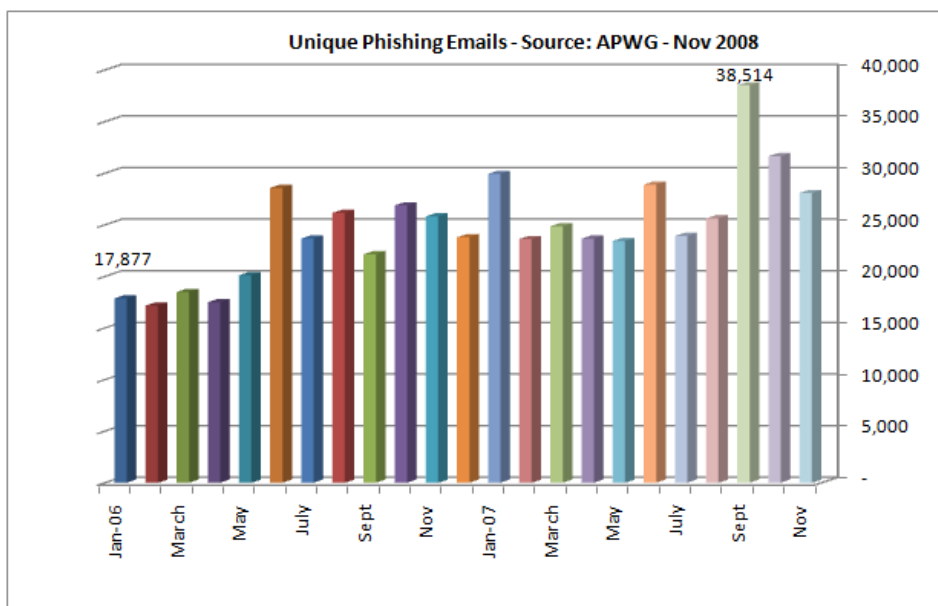


Figure 1. Phishing activity continues to increase (source: APWG 1/4/08 www.antiphishing.org).

Targeted Attacks: Spear Phishing and Whaling

Spear phishing targets specific individuals, groups, or employees of a company or organization rather than sending bogus e-mail messages to hundreds of thousands of unsuspecting users. These attacks are more personalized and sophisticated, and they are often more successful in inducing a target to part with sensitive information because of the message's relevance to the target.

For example, in late 2004 Microsoft employees were targeted in a spear phishing scheme involving e-mail messages that purported to come from a financial services company that administered employee 401(k) retirement programs. Timed to coincide with the end of a quarter when employees would

expect statements from this company, the spear phishing scheme launched an “address book” attack generating random employee names using the syntax of e-mail alias naming conventions used by Microsoft.

Had it succeeded, Microsoft employees might well have been deceived into thinking that the message was authentic and risked divulging personal financial information and access to their accounts. Fortunately, in part due to the implementation of the aforementioned Sender ID Framework, the forged e-mail messages were detected and deleted before delivery to users’ inboxes, and no Microsoft employee personal information was put at risk.

Starting in late 2007, whaling evolved as a sniper’s approach to phishing. Whaling is targeting specific high-net worth individuals or those deemed to have access to sensitive, confidential, and proprietary data. (The term *whaling* is derived from the term that casinos use to target high rollers.) Phishers have orchestrated cunning and elaborate exploits to target such users. Attacks (e-mail and Web site landing pages) are personalized based on information easily found from online searches and other public information.

Fooling Phishing Detectors

As phishers became more experienced with antispam efforts, phishers began to attempt to circumvent this protective technology by registering one domain—say www.bankphish.com—and then creating thousands of sub-domains, such as www.123.bankphish.com/login.html, www.234.bankphish.com/login.html, www.345.bankphish.com/login.html, and so on. Using this new tactic, phishers would evade phishing filters and send each of these URLs to a much smaller list of possible victims. By moving to the use of large numbers of sub-domains, phishers made it much more difficult to find and broadcast all known phishing sites to browsers and spam filters, so more of their messages were getting through.

Browser vendors and e-mail suppliers have countered this trend by blocking full domains—*.bankphish.com, say—instead of trying to block individual URLs used in a particular phishing attack. For organizations, this makes the proactive defensive registration of domain names (to prevent criminals from stealing them) and the detection of new phishing domains all the more critical.

Safeguarding Communications

By standardizing communications and letting customers know about e-mail and Web site policies, organizations can help customers better identify legitimate messages.

To avoid sending “phishy” e-mail messages, companies should follow these guidelines:

- Do not request personal information through e-mail.
- Personalize e-mail when possible.
- Do not redirect to another domain from the URL provided to customers.
- Do not rely on pop-up windows for data collection, especially those with no address bar or navigational elements.
- Do not use instant messaging or chat with customers unless they initiate the communication.
- Be explicit with “warning” and “immediate action required” communications.
- Let customers know what the company is doing to combat phishing.

By implementing these safeguards within the organization, businesses can help customers identify legitimate and illegitimate messages and build customer confidence.

TRUSTe and Ernst & Young have developed valuable guidelines that can help an organization shape and publish its policies regarding e-mail and sensitive information. The paper “How Not to Look Like a Phish” can be downloaded from TRUSTe at <http://www.truste.org>.

Password Checker: Check the strength of your password at www.microsoft.com/passwordchecker

Proactive Defense Strategies to Thwart Domain Infringement

There are many cost-effective steps an organization can take to help protect its reputation, assets, and customers. A range of third-party service providers can also help organizations combat and mitigate the risks posed by look-alike and phishing sites through a range of audit, monitoring, and professional services.

Microsoft uses a variety of strategies to help protect its own brands, assets, and customers and recommends them as a very effective approach to help thwart phishing and other domain infringement. These strategies include the following:

1. **Survey the Internet, identify risks, and monitor.** Your organization can start with an Internet survey that tracks down any look-alike or spoofed sites that might pose a threat to your brand, assets, or customers. Although it may not be possible to find 100 percent of such sites in this manner, it can help you detect a threat before deceiving your customers. You should consider establishing an ongoing relationship with a data protection service to help protect your online properties at all times and facilitate the rapid removal of identified phishing sites. A partial list is available at www.microsoft.com/safety/dataproviders.
2. **Survey your own organizational infrastructure and help eliminate vulnerabilities** by improving the security of (or hardening) your client computers and servers. Deploying an e-mail authentication system such as Sender ID Framework (SIDF) can improve security, as can e-mail applications and browsers with integrated anti-phishing technologies. *Organizations should also consider implementing DKIM as a complementary solution to be deployed with SIDF.*
3. **Formalize and widely publish policies concerning the collection of sensitive information through e-mail and the Web.** An organization should never ask anyone to provide personally identifiable information through e-mail, and it should strive to ensure that all its employees, customers, vendors, and partners know that they should not request sensitive information in this manner. That way, if a message requesting sensitive information arrives in a customer’s inbox and purports to be from the organization, the customer will know to be wary.

This last effort is critical because technology alone cannot be guaranteed to protect an individual or organization from phishing exploits. However, when technology and user education are combined, and when users know to be wary of any request for personally identifiable and sensitive information, both users and organizations are better able to avoid losses and to spot, report, and stop a phishing exploit quickly.

Survey the Internet, Identify Risks, and Monitor

Surveying the domain from a phishing defense standpoint involves conducting a worldwide inventory of Web sites that contain the product names of an organization, including those not registered or trademarked. It also involves surveying the Web for domain names that are similar to those owned by and associated with the organization.

Given the permutations of domain name spellings and domain types (such as .com, .net, .tv, .edu, and country-specific domain extensions), the number of possible Web sites are nearly infinite. However, by focusing on obvious look-alike sites—those that might easily deceive customers and those that a user might inadvertently visit by incorrectly typing a URL—the number of sites to examine will likely be much more manageable. Several third-party companies offer these and similar services, including other Internet brand protection services that can help an organization track usage of corporate logos and trademarked or copyrighted names.

Identify Risks

After an organization has identified the set of domains that could pose a risk to its customers and brand, it must determine which are real threats and which are not, and which domains can be easily acquired (and thus taken out of commission) and which cannot.

With the cost of domain registration falling below US\$10 per domain, it can be relatively easy and inexpensive for an individual or organization to register dozens of domain names. For many organizations, acquiring all the domain names associated with its company and products is some of the cheapest insurance it can buy.

Proactively Monitor for Phishing Sites

In addition to trying to take control of infringing domain names, an organization should consider retaining a service provider to perform proactive monitoring of new registrations to help ensure that new threats do not arise. This involves, in part, surveillance or monitoring of domains as they are registered, essentially keeping a lookout for domains that are obviously fraudulent.

Leading service providers include BrandProtect, Cyveillance, Digital Resolve, Internet Identity, MarkMonitor, NetCraft, and RSA. The organization can then choose to challenge the legality of the domain name registration or to monitor the site.

Building relationships with such firms in advance of any attacks and creating a notification form to submit to the company's Web site can save precious time and resources.

Improving Security Infrastructure

To help protect against data losses, an organization should do the following:

- Ensure that its Web sites, servers, and client computers are sufficiently protected (or hardened) to prevent easy takeover by a criminal looking to create a phishing site.
- Deploy inbound and outbound e-mail filtering and message authentication technologies—and require customers and business-to-business (B2B) partners to do the same—to create an even greater level of security within its broader communications ecosystem.
- Use standardized desktop configurations, complete with auto-updating mechanisms, and deploy the latest in browser-based anti-phishing technologies.
- Establish a relationship with a data reputation service provider. This provider can help maintain business continuity in a phishing attack and can help disseminate information about the phishing sites so that customers, employees, B2B partners, and others can avoid them.
- Implement Extended Validation SSL Certificates on sites that offer online transactions, including e-commerce and e-banking solutions. An EV SSL Server Certificate is a new category of SSL certificate created by the CA/Browser Forum, an industry consortium. This certification was created with a goal of increasing consumer confidence in online transactions. EV certificates are issued to Web sites only after rigorous validation of their identity. Web browsers will reflect this higher level of identity assurance with prominent and distinct trust indicators, such as the green address bar used by Internet Explorer 7.

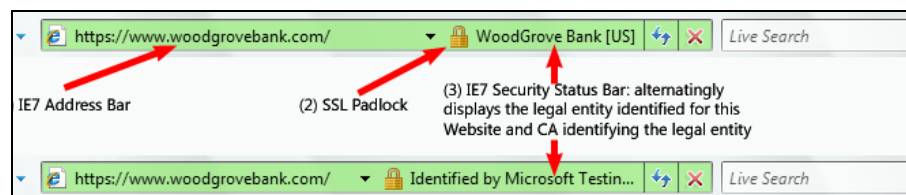


Figure 2. Internet Explorer 7 with EV SSL Certificates

- Use strong passwords on all computers and mobile devices, and require frequent changes. A strong password should appear to be a random string of characters. To create a strong password, follow these guidelines:
 - Make it lengthy. Each character increases the protection that it provides many times over. Passwords should be eight or more characters in length.
 - Combine letters, numbers, and symbols. The greater variety of characters, the harder it is to guess.
 - Use the entire keyboard, not just the most common characters. Symbols typed by holding down the Shift key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard and any symbols unique to your language.
- Data security on lost or stolen PC devices is a growing concern among security experts and corporate executives. The data stored and personal information on the PC asset is often significantly more valuable to a corporation than the asset itself. The loss, theft, or unwanted disclosure of that data can be highly damaging and has been estimated to be the source of nearly 50 percent of all identity thefts.
- BitLocker Drive Encryption is a data protection feature available in the Windows Vista® Enterprise and Ultimate editions for client computers and in Windows Server® 2008. BitLocker is the Microsoft response to this growing threat of information disclosure that can lead to loss of business confidential data and personal identity theft. By encrypting all data on the Windows volume, it addresses the threats of data theft or disclosure from lost, stolen, or inappropriately decommissioned personal computers. Deploying BitLocker is a best practice recommended for all mobile computers and any computer storing customer records or confidential data.

More SIDF

- Get more information, resources, and third-party solutions for e-mail authentication at www.microsoft.com/senderid.
- Create an SPF record by using the Sender ID Framework SPF Record Wizard at www.microsoft.com/senderid/wizard.

E-Mail Filtering, Authentication, and Sender ID

In response to e-mail exploits, Microsoft and several other industry leaders joined forces and created the Sender ID Framework (SIDF), an interoperable solution to help protect domain holders and users from misuse of their domain and brands. SIDF is a proven solution that can help protect an organization's domain from spoofing and phishing exploits while also improving the deliverability of the organization's legitimate e-mail. SIDF is now supported by more than 15 million domains worldwide, representing over 50 percent of all legitimate e-mail sent daily.

Organizations and ISPs can extend these capabilities by deploying an e-mail authentication solution. The leading choice is SIDF, which offers easy deployment and implementation with no costs or software updates required. Additional complementary approaches, such as DKIM, should be considered to provide comprehensive protection from e-mail spoofing.

Leading industry marketing and online safety organizations such as the Authentication and Online Trust Alliance (AOTA), BITS/Financial Services Round Table, Direct Marketing Association (DMA), the E-mail Sender and Provider Coalition (ESPC), the Interactive Advertising Bureau, and many service providers now require members to authenticate their domains and all outbound marketing e-mail.

SIDF seeks to verify that every e-mail message originates from the domain from which it claims to have been sent. As illustrated below, this is accomplished by checking the address of the server sending the mail against a registered list of servers that the domain owner has authorized to send e-mail. This verification is automatically performed by the Internet service provider (ISP) or recipient's mail server *before* the e-mail message is delivered to the user. The result of the SIDF check can be used as additional input into the filtering tasks already performed by the mail server. After the sender has been authenticated, the mail server may consider past behaviors, traffic patterns, and sender reputation, as well as apply conventional content filters, when determining whether to deliver mail to the inbox, junk e-mail folder, or quarantine folder or to block and delete it.

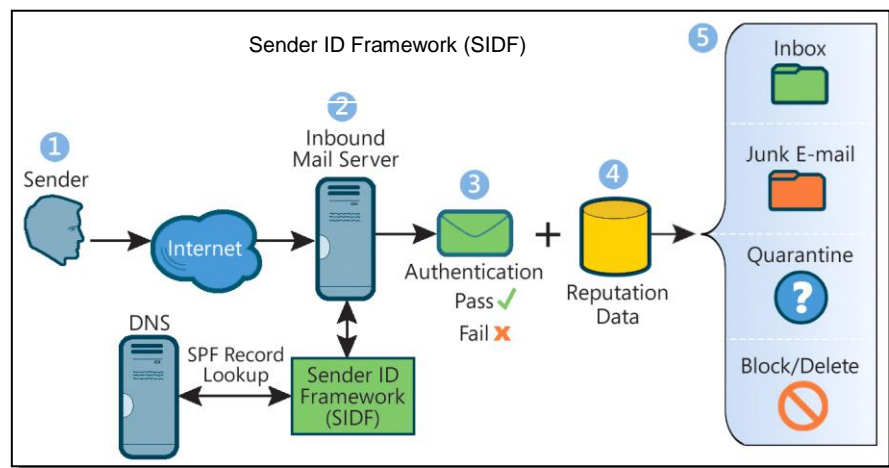


Figure 3. SIDF

All domain holders should ensure their outbound e-mail is SIDF compliant by creating and publishing a Sender Policy Framework (SPF) record in the zone file of their DNS. This will improve the deliverability and security of their e-mail. SPF records simply declare or list the IP address of servers authorized to send mail on the organization's behalf. Receiving network mail servers are able to compare the e-mail sent against this record to detect spoofing or phishing. Depending on the organization's e-mail systems and administrator protocols, such e-mail may be deleted, placed in a junk mail folder, or flagged with a warning to the user.

Harden External-Facing Servers

Free Lockdown Wizard

For organizations with Web sites based on Internet Information Services (IIS), Microsoft offers a free lockdown wizard. For more information, visit <http://support.microsoft.com/default.aspx> or <http://www.microsoft.com/technet/security>.

An organization can significantly reduce its vulnerability by hardening its Web sites and external-facing servers against a phishing attack. The organization can:

- Disable unused Web site services, ports, and default Web applications to reduce opportunities for intruders to gain access to its network.
- Ensure that the organization's Web site uses secure sockets layer (SSL) whenever customers and B2B partners are asked to provide sensitive information, and ensure that all digital certificates are accurate and current.
- Work with its Certificate Authority to acquire new Extended Validation (EV) SSL certificates, which can help provide stronger business validation and reassure consumers that they are not visiting a phishing Web site.
- Use digital signatures to validate the authenticity of e-mail messages sent from the organization.
- Check HTTP reference tags for all images to help catch phishing sites that are using the organization's logos and other images. One way to detect potential misuse of brand images is to compare the number of page views to the number of times an image has been served.
- Take a full accounting of all applications installed on the organization's servers and make sure that they are up to date with the latest security patches, antivirus definitions, and the like. Remove any default or testing applications that are not being updated.
- Install antivirus and antispysware tools on all servers, and use tools to perform complete scans monthly.
- Avoid using organizational servers to browse the Internet (even trusted sites) or to check e-mail. If possible, use computers other than servers to download vendor patches and similar content. Otherwise, limit downloads on servers to known sites only for vendor patches and similar functions.
- Deploy account login audit software to identify irregular usage behaviors such as repeated login failures or excessive logins from multiple networks.

- Regularly perform vulnerability testing to test the security of the organization's site. A variety of third-party vendors can provide these testing services regularly so that the organization can be more certain that its Web sites can withstand the latest methods of malicious users.
- Restrict access to internal servers and DNS systems with system log monitoring, and change logon credentials with every staff change.

Secure and Protect Computers

Not only should an organization tighten the defenses of its external-facing servers—it also needs to make sure that its client computers are healthy and well defended. Users should upgrade to the most current browser technologies, which offer dynamic protection from myriad threats, integrating phishing, privacy, and other threat prevention and detection technologies. Windows Internet Explorer 7 is the leading solution and the first to offer such enhancements. Internet Explorer is available at no charge at www.microsoft.com/ie.

In addition to Internet Explorer 7, Windows Live OneCare™ and Forefront™ client security can help protect computers from many different kinds of threats while also helping optimize the performance of user personal computers. To this end, all computers in the organization should:

- Be configured for automatic security and safety updates.
- Have their firewalls enabled.
- Run antivirus and antispyware applications and subscribe to services that keep these current.
- Have a full system scan run at least once each week.
- Have desktop software installed that prevents users from visiting known phishing sites and detects new phishing sites in real time.

In addition, organizations should consider outbound e-mail filtering. Organizations can also help fight phishing attacks by installing malware and spyware detection tools such as Microsoft Windows Defender, and they can encourage their customers to use it as well. Windows Defender is integrated in the Windows Vista operating system and is available free of charge to Windows XP users. Such malware and spyware detection helps protect the customer, but it also may prevent an attack on the organization's systems.

For example, a key logger application installed on a user's computer can record everything needed to steal the user's personal information as well as corporate logon credentials. No matter how many technical defenses an organization installs or how many server-based protections it deploys, client-side malware can easily compromise the integrity of an organization's systems.

More about the Microsoft Phishing Filter

- Read the white paper at www.microsoft.com/safety/phishing.
- Get the Microsoft Phishing Filter by downloading Windows Internet Explorer 7 from www.microsoft.com/windows/ie.

Use the Microsoft Phishing Filter

Another layer of defense enables the browser to play an active role in helping prevent users from browsing to known phishing sites. The Microsoft Phishing Filter is included in Windows Internet Explorer 7 for Windows XP SP2, Windows Server 2003, and Windows Vista.

The Microsoft Phishing Filter is an opt-in service that operates in the background while the browser is running. It relies on innovative browser-based heuristics to analyze Web pages dynamically and to warn users about suspicious characteristics as they browse, while ensuring that no personally identifiable information is stored or transmitted to Microsoft or any third party. Microsoft uses machine learning to continually update these heuristics and help keep the phish-fighting characteristics fresh. This client-side technology is combined with up-to-the-hour online information provided to Microsoft by a network of third-party data provider partners and a community of more than 200 million Internet Explorer users. Today, the Microsoft Phishing Filter successfully blocks nearly 1 million attempts to visit known phishing sites per week.

If the Phishing Filter finds a reason to question the integrity of a site, it provides the user with one of two warning levels:

- The first level of warning (associated with a yellow warning shield) tells the user that the requested URL is a “suspicious Web site” and recommends not entering any personal information on the site.
- The second level of warning (associated with a red warning shield) automatically blocks a user from a site if the URL has been confirmed as a reported phishing site by the phishing filter service. (Users can override this block, but it is not recommended.)

If the Microsoft Phishing Filter finds no reason to discourage the user from opening the site, it remains in the background, transparent to the user.

Enhancing Trust: Extended Validation SSL Certificates⁵

Historically Web site security has focused on protecting information in transit—helping keep information safe from prying eyes. Companies conducting e-commerce have adopted SSL certificates to help communicate to whom the site belongs, the domain to which the certificate was issued, and the country in which it was issued. The certificate sits on a secure server and is used to encrypt the data and to identify the Web site. Although SSL was designed to protect personal information from being accessed by third parties, online criminals have been able to obtain “valid” SSL certificates for their bogus sites. Some phishing sites have secured commonly misspelled domain names so that

⁵ Secure Sockets Layer (SSL) creates a secure connection between a client and a server. URLs that require an SSL connection start with *https*: instead of *http*:

users are less likely to notice the extra character in the address bar. It is important that users look for the gold padlock icon, but without the identity information users can still end up sending personal information to the wrong Web site.

In response to these threats, the CA/Browser Forum developed the Extended Validation (EV) SSL certificate, now adopted by more than 4,000 domains.⁶ EV certificates help increase online safety and security by consistently taking several extra steps to validate the business entity in addition to the certificate request. This comprehensive review and verification of a business's identity not only helps avoid certificates being issued to bogus sites, but also helps businesses protect their brand and users from being scammed.

EVs offer an improved level of authentication of entities that request digital certificates for securing transactions on their Web sites. Leading Web browsers, including Internet Explorer 7, display EV SSL-secured Web sites with a green address bar and lock, allowing visitors to instantly ascertain that a given site is indeed secure and can be trusted. This visual trust indicator provides the user with greater online confidence while enhancing the value to the domain holder's brand (see Figure 1).

EV SSL certificates are useful to any company that is conducting e-commerce and that desires to protect its brands from deceptive exploits. Leading sites that use this technology include Alaska Airlines, AutoZone, British Airways, eBay, FedEx, PayPal, Microsoft, Royal Doulton, The Body Shop UK, and Travelocity. In addition, leading financial services brands are realizing the benefits of EV SSLs, including the Banque National du Canada, Charles Schwab, Deutsche Bank, SunLife, Sovereign Bank, UBS, and Vanguard. EV certificates are used not only by large financial institutions, banks, and e-commerce sites, but also by charities and organizations such as the United Way and the Girl Scouts Hornets' Nest Council. More information is available at www.microsoft.com/windows/products/winfamily/ie/ev.

Engage with Data Reputation Vendors

Yet another layer of defense operates behind the browser-based anti-phishing technologies and SSL certificates just described. This is the network of data reputation vendors that work with companies to confirm and take down identified phishing sites. In addition to helping take down those sites quickly, a group of approved and accredited third parties also upload confirmed phishing sites into the Microsoft Phishing Filter reputation service and other similar services. This information is used to help block users from a newly discovered phishing site. If that site involves an organization's brand or Internet property, the rapid response these providers and the Microsoft Phishing Filter can deliver may make all the difference to the reputation of the brand and the safety of customers and partners.

⁶ Source: Netcraft - January 2008

Reputation vendors that provide phishing information to the Microsoft Phishing Filter service include BrandProtect, Cyveillance, Digital Resolve Internet Identity, MarkMonitor, Netcraft, and RSA Security Inc. Additional third-party data providers are being evaluated to maximize worldwide coverage. Every business that is considering taking advantage of the enhanced protection afforded by these data reputation providers should consider developing relationships with them now—even businesses that are not aware of any current phishing exploits involving their sites or brands. Doing so may help the business respond without delay should such an exploit occur in the future.

A summary of service providers is available at www.microsoft.com/safety/dataproviders.

Case Study: The Microsoft Experience

This case study demonstrates the breadth and depth of issues related to protecting domain names, and how businesses can apply these lessons to build the domain defense strategy. This strategy has five elements:

1. Identifying problem domain names
2. Securing those domains
3. Proactively monitoring domain names and Web sites
4. Observing dangerous trends
5. Proactively seeking spoof sites

Identifying Problem Domain Names

Microsoft surveyed its domain to combat the risks posed by look-alike Web sites. (Microsoft must monitor a large number of brands, including Microsoft Office, the Windows Live Hotmail Web-based e-mail service, the Xbox 360[®] video game system, and the Windows operating system.) It began by identifying domain names that could be used to fool customers into believing that the domain was owned and operated by Microsoft. The company worked with an Internet brand protection company, which compiled a comprehensive list of domain names that had previously been used against Microsoft and other companies.

Then Microsoft applied its analysis to come up with other name combinations that might easily fool a user, producing a list of more than 500 unique domain names that, once applied across the six generic top-level domains (.com, .net, .org, .biz, .info, and .us), grew to more than 3,000 domain name permutations. It then determined which names were already owned and registered and which were not. After this analysis was complete, the results were segmented into the following categories:

- Domain names owned by Microsoft
- Domain names available for purchase
- Domain names owned by others

The third category clearly posed the most risk to Microsoft and its customers, so Microsoft further broke it into two subcategories:

- Domain names owned by cyber-squatters
- Domain names owned by unfamiliar people

Securing the Domains

Microsoft launched a plan to secure all the domain names on its list to minimize the risk of phishing attacks.

Category 1. For domains already owned by Microsoft, it made sure registration of the names was ensured for several years, placed them on auto-renew, and also placed them on a watch list to help ensure that its ownership of the names did not inadvertently lapse into the hands of a drop-catch. A vendor operating in this capacity can also be authorized to renew the domain names on a client's behalf, but many large companies—including Microsoft—already have a domain team to handle such registrations.

Category 2. Microsoft purchased all the domain names that could be readily acquired and secured the registration rights in the same manner as the domains previously owned.

Category 3. Microsoft decided on a soft approach for domain names owned by others and sent all the owners a letter requesting they transfer the domain name to Microsoft. In compensation, Microsoft offered a fee that would have covered the purchase price of a replacement domain name and any transfer fees.

There were several responses:

- Several owners agreed immediately and relinquished the domain names in question.
- Others refused this offer or responded with requests for exorbitant amounts of money. These owners were referred to the Microsoft trademark division for investigation and possible enforcement actions.
- Still others never responded. Microsoft then contacted the domain name registrars and asked them to confirm the registration information, per Internet Corporation for Assigned Names and Numbers (ICANN) regulations.

These remaining domain names were added to a quick recovery list in the event they are allowed to expire. Doing so have allowed Microsoft to successfully obtain the majority of those outstanding.

Although not every company has the global reach and product breadth of Microsoft, this approach works for many organizations. No domain name protection program will cover every conceivable look-alike domain name, but when a company raises its defenses, the criminals might pursue softer targets, such as companies that have not taken such preventive measures.

Proactively Monitoring Domain Names and Web Sites

While working on the defensive domain name purchases, Microsoft launched a proactive domain name monitoring program. The vendor that watches the company's domain name expiration dates also monitors new domain name registrations. Microsoft regularly reviews this for domain names that might be used to defraud customers. These domain names are then added to a watch list, and the sites—numbering more than 15,000—are routinely monitored for activity.

Microsoft has immediately challenged registrants that use fraudulent Microsoft credentials or use malicious names in conjunction with Microsoft product brands. Domain name registrars have an obligation under ICANN to take action upon receipt of a formal challenge. To date, Microsoft has challenged and disabled more than 2,000 phishing related Web sites targeting Microsoft, MSN[®], and Hotmail users since January 2004.

One such example of an infringing domain name is windowsmessenger.com. This direct navigation domain is not the genuine home page for the Microsoft Windows Live Messenger service. However, it was registered by a third party and subsequently used to monetize visitor traffic by using the Google AdSense program. This cyber squatting against the genuine Microsoft Web site negatively impacted the Microsoft brand and reputation. After contacting the domain name registrant and challenging his actions, the Microsoft Domain Defense enforcement program recovered the name plus other relief in late 2007. Microsoft now is redirecting visitor traffic from this site to the genuine Windows Live Messenger home page. This example illustrates the importance of robust domain name portfolio monitoring and enforcement, and understanding how your customers interact with your Web site—and your brand—online.”

Observing Dangerous Trends

Real-time domain name monitoring has also enabled Microsoft to notice domain name registration trends. By observing a sudden increase in the registration of domain names that clearly target other companies, Microsoft has been able to recognize the registration name pattern and proactively secure those domain names before they could be registered by attackers. For example, in one case Microsoft observed the registration of certain domain names that used a pattern involving well-known Internet brands combined with a hyphenated wild-card term such as “Brand A - xxxx,” “Brand B-xxxx,” and so on. Shortly thereafter, Microsoft also observed phishing attacks that used those domain names. In response, Microsoft quickly registered domain names that use similar wild-card combinations (such as “Microsoft - xxxx”) to prevent an attacker from using them.

Proactively Seeking Spoofed Sites

As an additional layer of defense against phishing and malware-related sites and Web pages, Microsoft has engaged a third-party company to search the Internet around the clock in pursuit of sites that use Microsoft logos and brand treatments or that mimic sign-in pages that are associated with Microsoft properties. Ninety percent of the phishing sites that spoof MSN, Windows Live Hotmail, and MSN Hotmail have been located through this approach.

There are other techniques that brand owners can consider to monitor for phishing sites:

- Any ISPs (AOL, MSN, Yahoo, and the like) or company can set up “trap” accounts without antivirus or antispyware protection and monitor the e-mail those accounts attract. These e-mail messages can be used for technical analysis, and can also potentially be used in law enforcement actions.
- The company can set up a trap account on an unprotected computer (known as a *honey pot*) at the organization’s IP address. IT staff can then track the e-mail that the computer attracts, looking for links to Web sites that attempt to spoof the company’s site.
- The company can use a browser such as Internet Explorer 7 that provides dynamic anti-phishing tools. These tools not only pinpoint known phishing sites, but, using heuristics, can also identify potential phishing sites.

ROI: Phishing Exploits Decrease by 80 Percent

Such efforts clearly work. Through a proactive campaign to acquire look-alike domain names and to find and eliminate look-alike and phishing sites, an organization can make it costlier and more difficult for phishers to succeed. This can prompt phishers to look for easier targets elsewhere. According to Microsoft internal data, through the use of these combined approaches, including initiating more than 14,000 take down notices, domain name–based phishing attacks against Microsoft dropped by over 80 percent. To further protecting the Microsoft brand, Microsoft has supported more than 565 enforcement actions worldwide against spammers, phishers, and spyware and other malicious code distributors. These actions include civil lawsuits in the United States as well as assistance to law enforcement officials around the world in bringing prosecutions against online criminals.

What to Do If Compromised

How to Protect Your Identity and What to Do If Your Identity Is Stolen

The U.S. Federal Trade Commission offers some advice to individuals who suspect that they are receiving phishing e-mail or have been the victim of a phishing exploit:

- **Review credit card and bank account statements as soon as they are received** to check for unauthorized charges. If a statement is late by more than a couple of days, call the credit card company or bank to confirm the billing address and account balances.
- **Order a free copy of credit reports periodically** from any of the three major credit bureaus. If an identity thief is opening credit accounts in their name, these new accounts are likely to show up on these reports. Get details on how to order a free annual credit report at www.annualcreditreport.com.
- **Forward spam that is phishing for information** to spam@uce.gov and to the company, bank, or organization impersonated in the phishing e-mail. Most organizations have information on their Web sites about where to report problems.
- Follow the instructions at the FTC's Identity Theft Web site, www.ftc.gov/bcp/edu/microsites/idtheft/. Victims of phishing can become victims of identity theft.

You can download more information about how to avoid phishing from the FTC site: www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf.

Phishing exploits that succeed in collecting sensitive information may lead to theft of customer identities, financial information, and confidential corporate data. These can reduce an organization's ability to conduct business online.

Creating an Incident Response and Disaster Plan

Any organization that relies on the Web for commerce and customer communications should have contingency plans for phishing attacks and compromised accounts. We recommend creating a cross-functional response team with representatives from sales, marketing, public relations, and information technology to deal with phishing and other online attacks before they happen. The response team's responsibilities should include:

- Creating a plan for dealing with any phishing attack. Consider engaging a data protection provider, a company that's expert at shutting down phishing sites. These vendors have the experience and contacts with ISPs, registrars, and others that enable them to shut a site down much faster than you would be able to—often within hours of its detection. A list of data protection providers who are Microsoft partners is available at www.microsoft.com/safety/dataproviders.
- Developing contacts at your registrar, hoster, and ICANN, and understanding their processes, policies, and procedures.
- Arming the sales and PR teams with response plans and policy statements.
- Providing speaking points for customer service agents who will field customer phone calls.
- Developing "on hold" messages for the organization's call centers to inform customers about the attack while they are waiting to speak to a customer service representative.
- Setting up a system that monitors all server logs and creates audit trails, including capturing screen shots and caching of suspicious pages.
- Ensuring that decision-makers responsible for network security and the brand are available at all times.
- Creating a Web page to be used as a redirect when a phishing site is taken down. Doing so can provide users with prescriptive advice and confidence that you have eliminated a potential threat. The Authentication and Online Trust Alliance (AOTA) has sample text at www.aotalliance.org/resources/samplephishpage.html.

- Creating e-mail aliases with names such as “abuse,” “phishing,” and “fraud” at the company’s e-mail address—for example, fraud@contoso.com.
 - Encouraging customers, vendors, and partners to report any suspected attacks or abuses of the company name or brand.
 - Monitoring aliases at all times, 365 days a year. Phishers and scam artists do not work a standard business-hour day and often plan a phishing attack to start late on a Friday afternoon so they can phish for data undetected—or at least unreported—the entire weekend.
- Being aware of the local legal situation and the resources available to assist the team. Local, state, and federal laws may influence both an organization’s response and which parties can help it, and these laws can be convoluted.
- Reviewing the company’s insurance policy for coverage on losses due to phishing attacks and business continuity coverage.

Responding to Incidents

According to the Anti-Phishing Working Group (APWG) and Microsoft research, the average life of phishing sites is now three days, with the full range stretching from a few hours to a few weeks. Criminals have also been known to take down their own phishing sites after a period of time to avoid detection, and then restore the site later for a second wave.

If an organization discovers that it has been compromised, here are the steps we recommend:

- As soon as you become aware of a phishing site, initiate take-down procedures. Many Web hosting companies and ISPs will readily cooperate with such a request when presented with sufficient evidence of malfeasance. Contact hosting companies and ISPs, not the “owner.” With phishing sites, the original registrations often turn out to have been made with stolen credit card numbers and registered with false information. This by itself provides sufficient grounds for both shutting the sites down and reregistering the sites in the organization’s own name (thus making the sites unavailable to con artists for phishing expeditions).
- Contact the data protection provider if you’ve retained one. If not, formally notify the registrar, Domain Name System (DNS) provider, hosting company, Internet service provider (ISP), and the registered owner of the offending Web site, requesting that they take the site down. Notify these parties by telephone, fax, and e-mail (using Read and Delivery Receipt) to document the request. Ask that they retain any logs or registration information.
- Warn your customers as quickly as possible of the phishing attack.

- In writing and by phone, contact customers who have been placed at risk. Reiterate that your company does not and will never send links in e-mail requesting password or account information. Ask them to change passwords, not reveal their passwords, and possibly close their accounts.
- Consider placing a fraud alert on your organization's home page and online sign-in screens to alert visitors to the threats. Provide them with information about how to get assistance or more information, including a toll-free phone number.
- Give customer service the details of the attack so that they can reassure customers who report an attack that they are aware of and dealing with the potential threat.
- If your organization is not successful in taking down the alleged phishing site, it should analyze the HTML code of the site to:
 - Look for image references on the phishing site that actually point to the legitimate site. Update the legitimate site to use new images, and update the old images with a warning to the user. That way, when those images appear on the phishing site, the warning images may alert the visitor.
 - Identify where phished information is being sent. Notify the ISP or e-mail provider whose services are being used to collect information of the exploit and ask them to keep any related logs. Give this information to the appropriate law enforcement agencies.
 - Notify the Internet Crime Complaint Center (www.ic3.gov) or the appropriate law enforcement agency in its area. In addition, submit data to the Anti-Phishing Working Group for data tracking at www.antiphishing.org/report_phishing.html.
- If you can identify suspect sites (either by identical or similar registration information), you can also ask the registrar to remove these domains proactively. Even if there is no evidence that these sites have yet been used in phishing exploits, the similarities to phishing sites that have gone live are often sufficient grounds to request removal of the site as a preventive measure.
- After the site has been rendered inoperative, try to acquire the domain name so that it cannot be reused.

Conclusion

There is much that an organization can do to protect its assets, brands, and customers, whether on its own or in partnership with third-party vendors. For example, an organization can:

Prescriptive Advice for Users

Microsoft has created a series of brochures about online safety topics, including phishing, identity theft, spam, and keeping children safe online. These materials can be reproduced and distributed free of charge to an organization's employees and customers. Find them at www.microsoft.com/security.

Information and resources for IT professionals and business is available at www.microsoft.com/safety.

- Upgrade all client personal computers to run Internet Explorer 7, and enable the Microsoft Phishing Filter (available from the **Tools** menu; click **Phishing Filter**, and then click **Turn On Automatic Checking**).
- Educate employees and customers about ways to protect themselves from phishing and other exploits and ways to identify legitimate e-mail and Web sites associated with the organization and its activities.
- Complete an inventory of the domain names that it owns, and audit how many it should own, given the permutations that could create risk for the organization, reputation, employees, and customers. Then, the organization should acquire as many of these domain names as possible.
- Monitor new domain name registrations to watch for any new domains that may pose risks.
- Create an incident response team and disaster plan, and establish IT policies for auditing server activity and maintaining log files in case of a security breach.
- Harden external-facing servers and client computer systems.
- Deploy Sender ID to authenticate inbound and outbound e-mail and consider DomainKeys Identified E-mail (DKIM) as part of its e-mail security strategy.
- For commerce and transactional data sites, upgrade existing SSL Certificates to the EV SSL Certificates as certificates come up for renewal.
- Where possible, activate Windows BitLocker to encrypt hard disks, protecting personal computers from physical data theft.
- Consider developing a relationship with a data monitoring and reputation vendor such as Return Path or Habeas, or a third party that provides data feeds into the Microsoft Phishing Filter reputation service such as Brand Protect, Cyveillance, Digital Resolve, Internet Identity, MarkMonitor, Netcraft, or RSA Security

Although none of these efforts is foolproof and none will stop every attempt to collect sensitive information or compromise a site, the combined resistance these steps create may be sufficient to discourage Internet criminals from pursuing their aims with an organization, its employees, or its customers. Ultimately, most information thieves want to collect their prizes with as little effort as possible. If an organization mounts a strong defense, criminals will often seek out other organizations and sites that are not as strongly protected.

References

The following sites offer more information about tools, technologies, and procedures that can help an organization protect itself and its brands.

U.S. Chamber of Commerce	www.uschamber.com/sb/security
Anti-Phishing Working Group (APWG)	www.antiphishing.org
Authentication and Online Trust Alliance (AOTA)	www.aotalliance.org
CA/Browser Forum	www.cabforum.org
Direct Marketing Association (DMA)	www.the-dma.org
Federal Trade Commission (FTC)	www.ftc.gov www.ftc.gov/ftc/cmplanding.shtm
Internet Corporation for Assigned Names (ICANN)	www.icann.org
Internet Crime Complaint Center	www.ic3.gov
Sender ID Framework	www.microsoft.com/senderid
TRUSTe	www.truste.org

Microsoft Safety and Security Downloads

Microsoft security resources	www.microsoft.com/security www.microsoft.com/safety www.microsoft.com
Windows Vista	www.microsoft.com/vista www.microsoft.com/vista/bitlocker
Windows Internet Explorer 7	www.microsoft.com/ie
Microsoft Phishing Filter	www.microsoft.com/safety/phishing
Microsoft TechNet security tools	www.microsoft.com/technet/security/tools

Information Updates

As spam, phishing, and other criminal tactics evolve online, updated versions of this white paper will be available at www.microsoft.com/safety in “Technology Focus” or www.uschamber.com/sb/security in “Cyber Security Advocacy.”