

Protecting Your Business & Brand from Online Threats

Prescriptive advice a business can use to
protect its domain, customers and assets

White Paper

April 2007



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 some best practices and general recommendations for businesses of all sizes. While 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), Direct Marketing Association (DMA), E-mail Sender and Provider Coalition (ESPC), Federal Trade Commission, International Association of Privacy Professionals (IAPP), TRUSTe and U.S. Department of the Treasury. The authors would also like to thank Laura Mather - Mark Monitor, Rod Radmussen - Internet Identity, Michael Chadwick - GoDaddy.com, Aaron Kornblum - Microsoft and Michael Zanies from the Interactive Advertising Bureau, for their valuable insights and perspectives.

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, MSN, Hotmail, Xbox, Windows, Windows Live and Outlook 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.

© 2007 Microsoft Corp. All rights reserved.

Contents

Introduction	1
Evolution of Domain Infringement	2
Domain Squatters.....	2
Drop-Catching	3
Domain Kiting	3
Domain Spoofing and E-mail Forgery	4
Spear Phishing	6
Fooling Phishing Detectors	6
Proactive Defense Strategies to Thwart Domain Infringement	7
Survey the Internet, Identify Risks & Monitor	8
Identify Risks.....	8
Proactively Monitor for Phishing Sites	8
Improving Security Infrastructure	9
E-Mail Filtering, Authentication & Sender ID.....	10
Harden External-Facing Servers.....	11
Secure and Protect Computers.....	12
Use the Microsoft Phishing Filter	13
Engage with Data Reputation Vendors.....	13
Case Study: The Microsoft Experience	15
Identifying Problem Domain Names.....	15
Securing the Domains	16
Proactively Monitoring Domain Names & Web Sites	17
Observing Dangerous Trends	17
Proactively Seeking Spoofed Sites	17
ROI: Phishing Exploits Decrease by 80 Percent.....	18
What To Do If Your Brand Has Been Compromised	19
Creating an Incident Response and Disaster Plan	19
Responding to Incidents.....	20
Conclusion	22
References	23

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's brand or reputation will be compromised by criminals
- Less risk to individuals who might inadvertently publicize sensitive information
- Greater confidence that communications from an organization is legitimate
- Increased deliverability and reliability of legitimate e-mail
- Gain a competitive advantage

Products and Technologies

- Microsoft Internet Explorer 7
- Microsoft Phishing Filter
- Sender ID Framework

Introduction

The Internet and e-mail have become a vital platform for communication, productivity and commerce. The combination of RSS feeds, instant messaging, e-mail and the Web has created new markets and opportunities for businesses of all sizes and across all vertical markets. 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.

According to the 2007 Identity Fraud Survey Report released by Javelin Strategy and Research, nearly ten million adults were affected by identity theft, incurring a combined loss to themselves and business in excess of \$40 billion, yet the majority of these have been unrelated to the Internet. In the 2006 Internet Crime Report published by the FBI, they report internet related complaints actually decreased 10.4% in 2006 over 2005. While only a small percentage of identity theft has been attributed to online exploits, user perceptions are the opposite. 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 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 with a substantial Web presence, approaches these threats. Incorporating valuable 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 there are other security and safety threats beyond the scope of this paper, this paper focuses primarily on threats that specifically affect a business's brand and customers through deceptive e-mail, phishing exploits and unscrupulous domain registration practices, including domain squatting and drop-catching.

Authors:

Craig Spiegle
Director,
Online Safety Technologies & Practices
Microsoft Corporation

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

Evolution of Domain Infringement

In the late 1990s, Microsoft first began to experience a variety of online challenges to its brands and trademarks. Web sites began to appear that relied on look-alike domain names. These sites spoofed Microsoft and deceived customers by marketing and selling gray-market and counterfeit products; some published deceptive information about Microsoft, its products, its directions and its intents. Each site effectively compromised Microsoft's image, its brands and its reputation—to say nothing of the revenues lost to fraudulent software sales. 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 is now referred to as “domain squatters,” “typo-squatter,” or “cyber squatters,” individuals and businesses who have registered domain names with the goal of “ransoming” them to the brand owner. 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, where a “microsoft” is misspelled, due to a typing error and the user omitting 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 brand or trademark owners, but the legal costs and time can easily outweigh the cost of just buying the domain name, which works in the domain squatter's favor.

It has been estimated by VeriSign, that more than 500,000 domains have been registered solely for the purpose of trying to extort money from companies that want to protect their brands and trade names. While this is less than one percent of all of the domains registered worldwide, this 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.

Each organization has to determine what the business impact could be in the case of domain squatters owning or using look-alike domain names. There are legitimate reasons for an organization to own and operate a domain where the only difference between [www.\(YourCompanyName\).com](http://www.(YourCompanyName).com) is [www.\(YourCompanyName\).net](http://www.(YourCompanyName).net) and others.

To help protect from these exploits, brand owners should complete regular 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 both recover the names and potential profits made through profiteering. As companies and brand owners have successfully increased defenses from this exploit, the cyber squatters have evolved, targeting existing high traffic domains which expire via 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 due to the limited number of words and terms that are left unregistered, and that many names have been abandoned as a result of the .com bust, leaving valuable names to expire. Further creating this "opportunity," thousands of domains 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 often 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 before expiration.

Even though a company may have gone out of business or a product has been 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 DN Journal (<http://dnjournal.com>), in early 2007, such domains have been re-sold for upwards of \$1 million.

Domain Kiting

Domain kiting exploits an ICANN regulation that allows a domain owner to return a domain within five days for a full refund. The owner of the domain can 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 there, the site owner cashes in on the click-through.

A recent Mark Monitor (<http://www.markmonitor.com>) study showed that domain kiting represents large percentages of the domains registered in association with brand names. This study reviewed a major US based financial institution, evaluating all of the domains registered that contained their name, finding over a 1,000 related domains. They found 21.5% of the domains hosted pay-per-click pages, taking advantage of domain kiting. The largest percent of the domains (70%) no longer had any company content on the resulting Web pages indicating 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" 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 the more common tactic of "stealing" personal information and log on credentials. Since the "from address" corresponds to a trusted brand, the user is more likely to trust the e-mail, open it and click to the deceptive Web site and risk becoming a victim of online fraud.

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 message might arrive from what wrongly appears to be a legitimate business, usually a well-known brand name and Web site. For example, a message might inform the recipient that the company has evidence that someone had been trying to tamper with his or her bank account, and regulations now required the user to log onto the Web site to change his or her password. Other common examples include sending users an e-mail to log onto 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, the user lands on a Web site that appears identical to the bank's legitimate Web site. The user would then be 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. Once the user presses the Enter key, the bogus site would present an official-looking page that confirms acceptance of the new password and assures the user that everything would then be fine.

But, of course, it would not be 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 realized what had happened, the criminals had 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 continue to climb, with a year over year growth of over 50%. This growing threat is no longer limited to Fortune 500 Web sites. It has now 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 which puts a user's computer at risk by just visiting the site. The malware's sole intention is to capture confidential personal and business information.

These blended threats also have included scripting code that turns an unprotected PC 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 would suggest.

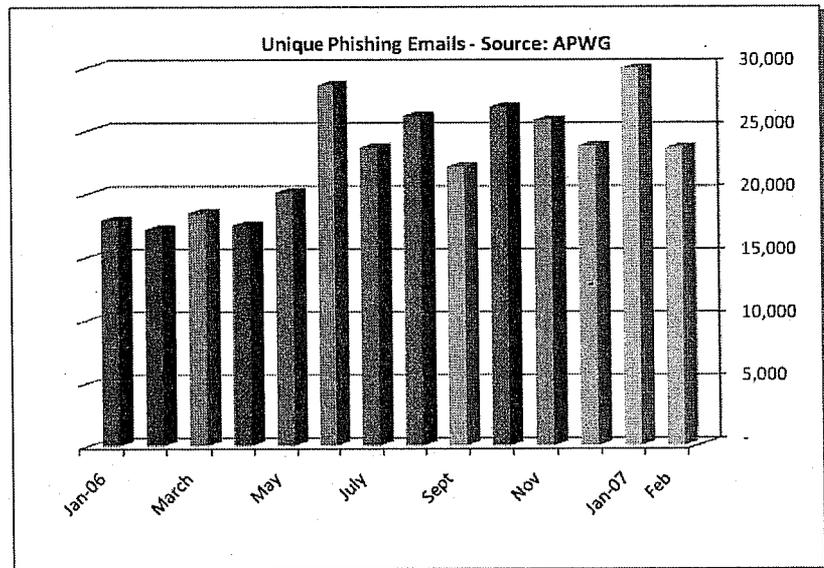


Figure 1. Phishing activity continues to increase (source: APWG 4/1/2007 www.antiphishing.org).

Spear Phishing

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 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 which 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 fraudulent message was authentic and clicked through to a Web site where they would have been at risk of giving away critical information. 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.

Fooling Phishing Detectors

As phishers became more experienced with anti-spam efforts, phishers began to attempt to circumvent this protective technology by registering one domain—say www.bankphish.com—and then creating up to thousands of sub-domains—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—www.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 of their e-mail and Web site policies, organizations can help customers better identify legitimate messages.

To avoid sending "phishy" e-mails, companies should follow these guidelines:

- Do not request personal information from customers via e-mail.
- Personalize e-mail when possible.
- Do not redirect to another domain from the URL provided 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>.

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 via 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. You should consider establishing an ongoing relationship with a data protection service to help protect your online properties 7x24 and facilitate the rapid removal of identified phishing sites.
2. **Survey your own organizational infrastructure and help eliminate vulnerabilities** by improving the security of (or hardening) its client computers and servers. Deploying an e-mail authentication system such as Sender ID framework can improve security, as can e-mail applications and browsers with integrated anti-phishing technologies.
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 it 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 the user knows to be wary of any request for personally identifiable and sensitive information, both users and organizations are better postured to avoid losses and to spot, report and stop a phishing exploit quickly.

Survey the Internet, Identify Risks & 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 which might easily deceive customers and those which a user might inadvertently visit by typing a URL incorrectly—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

Once 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 \$10 (U.S.) 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 the domain names that could pose problems, an organization should also perform proactive monitoring 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.

Again, there are third parties that provide this kind of monitoring service, and they can alert an organization immediately if someone registers a domain name that could pose a threat to the organization's business or its customers. The organization can then choose to challenge the legality of the domain name registration or to monitor the site.

Many third-party firms also offer services to monitor the Internet for sites that spoof an organization's pages—an account login page, for example. They can quickly alert the organization if they discover that someone has built a page that customers or employees might mistake for one of the organization's own if they were directed there through a phishing scheme. Building relationships with such firms in advance of any attacks and creating a notification form to submit to the company's Web site so they can save precious time and resources.

Improving Security Infrastructure

To help protect against the losses that can arise from phishing exploits, organizations 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 e-mail filtering and message authentication technologies—and encourage 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 customers, employees, B2B partners and others can avoid them.
- Implement EV SSL Certificates sites offering online transactions including e-commerce and e-banking solutions. An Extended Validation (EV) SSL Server Certificate is a new category of SSL certificate created by an industry consortium called the CA/Browser Forum. This new category of certification was created with a goal of increasing consumer confidence in online transactions. EV certificates will be 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 Microsoft Internet Explorer 7.

More SIDF

- Get more information, resources, and third-party solutions for e-mail authentication at www.microsoft.com/senderid.
- To create an SPF record at www.microsoft.com/senderid/wizard.

E-Mail Filtering, Authentication & Sender ID

Responding to this exploit, 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 which can help protect an organization's domain from spoofing and phishing exploits, while improving the deliverability of the organization's legitimate, e-mail. SIDF is now supported by over 8 million domains worldwide.

Organizations and ISPs can extend these capabilities by deploying an e-mail authentication solution. The leading choice is the Sender ID Framework, (SIDF), offering easy deployment and implementation with no costs or software updates required. Additional complementary approaches, such as DomainKeys Identified Mail (DKIM), are emerging that may warrant consideration depending on an organization's e-mail infrastructure and use case scenarios.

Leading organizations such as the Direct Marketing Association (DMA) and the E-mail Sender and Provider Coalition (ESPC), and many service providers, now require members and users to authenticate all outbound marketing e-mail.

The Sender ID Framework (SIDF) seeks to verify that every e-mail message originates from the Internet 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 Sender ID check can be used as additional input into the filtering tasks already performed by the mail server. Once 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, quarantine or block and delete.

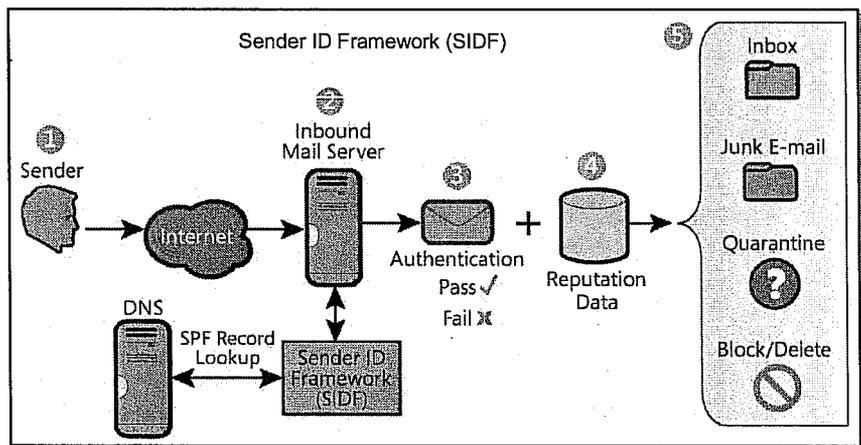


Figure 2

All domain holders should insure 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 completely deleted, placed in a junk mail folder, or flagged with a warning to the user.

According to research conducted by MarkMonitor, the Sender ID Framework is a leading protocol used by nearly eight million domain holders and protecting more than one billion e-mail users around the world. Sender ID authenticates more than 40% of legitimate e-mail sent across the Internet each day. More than 25 percent of Fortune 500 companies support it as a best practice, including Microsoft, which, through its Windows Live Hotmail service, was one of the first organizations to deploy Sender ID worldwide. More information on this open source / GPL compatible, royalty free standard is available from www.microsoft.com/senderid and the Authentication and Online Trust Alliance www.aotalliance.org

Harden External-Facing Servers

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.
- To help prevent phishing sites from using your logos and other images, check HTTP reference tags for all images.
- 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 antispyware tools on all servers, and use tools to perform complete scans monthly.

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>.

- 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 your site. A variety of third-party vendors can provide these testing services regularly so you're more certain that your organization's Web sites can withstand the latest methods of malicious users.
- Restrict access to internal servers and DNS systems, with system log monitoring, changing log on 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. (Microsoft offers a comprehensive service, Windows Live OneCare, that can help protect computers from many different kinds of threats. Forefront, an enterprise antivirus client, is also in the works.) 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.
- Run full system scans at least once each week.
- Install desktop software that prevents users from visiting known phishing sites and detects new phishing sites in real time.

Organizations can also help fight phishing attacks by installing malware detection tools such as Microsoft Windows Defender and encourage their customers to use it as well. Not only does this help protect the customer, but it may prevent an attack on the organizations' 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 Microsoft Windows Internet Explorer 7 from www.microsoft.com/windows/ie.
- Download the free MSN Search Toolbar from <http://addins.msn.com>.

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 Microsoft Windows® XP Service Pack 2, Windows Vista™ and the Windows Live Toolbar.

The Microsoft Phishing Filter is an opt-in service that operates in the background while the browser is running. It relies on new, innovative browser-based heuristics to analyze Web pages dynamically and warn users about suspicious characteristics as they browse. 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 over 100 million Internet Explorer and Windows Live Toolbar users. Today, the Microsoft Phishing Filter successfully blocks over 1 million attempts to visit known phishing sites per week.

If the Phishing Filter finds a reason to question the integrity of the 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.

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.

Engage with Data Reputation Vendors

Yet another layer of defense operates behind the new browser-based anti-phishing technologies 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, where it can 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.

Reputation vendors currently providing confirmed phishing information to the Microsoft Phishing Filter 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 in the months ahead. 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.

An updated list of such companies is available at <http://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 which has five elements:

- Identifying problem domain names
- Securing those domains
- Proactively monitoring domain names and Web sites
- Observing dangerous trends
- 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, among others.) 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 of criminal enterprises to the list 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. Once 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, 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-catcher. Microsoft's vendor contacts the company several months before the expiration of a domain name registration, which helps ensure that there is plenty of time to renew ownership. 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. Microsoft has obtained several of these domain names in this manner.

While 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 & 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 names such as "Hacker." 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 2000 phishing related Web sites targeting Microsoft, MSN and Hotmail users since January 2004.

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 using 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 login pages associated with Microsoft properties. Ninety percent of the phishing sites that spoof MSN, Windows Live™ Mail, 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 mails can be users for technical analysis as well as potentially utilized in law enforcement actions.
- The company can set up a trap account on an unprotected machine (known as a *honey pot*) at the organization's IP address. IT staff would then track the e-mail that machine attracts, looking for links to Web sites that attempt to spoof the company's site.
- Use a browser such as Windows Internet Explorer 7 with 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, in turn, has prompted them to look for easier targets elsewhere. According to Microsoft internal data, through the use of these combined approaches, domain name-based financial phishing attacks against Microsoft dropped by over 80 percent in 2005, while phishing exploits in general increased dramatically during the same period.

What To Do If Your Brand Has Been Compromised

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

The U.S. Federal Trade Commission offers several pieces of 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/ as victims of phishing can become victims of identity theft.

More information about how to avoid phishing is available from the FTC at www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf.

Phishing exploits that succeed in collecting sensitive information may lead to theft of your customer's identities, financial information as well as confidential corporate data, resulting in diminishing 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 functionalities to deal with phishing and other online attacks before they happen. The response team would:

- Create 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 allow them to shut a site down much faster than you would be able to—often within hours of its detection. You'll find a list of data protection providers who are Microsoft partners at www.microsoft.com/safety/dataproviders.
- Develop contacts at your registrar, hoster and ICANN. Understand their processes, policies and procedures.
- Arm the sales and PR teams with response plans and policy statements.
- Provide speaking points for customer service agents who will field customer phone calls.
- Develop "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.
- Set up a system that monitors all server logs and creates audit trails, including capturing screen shots and caching of suspicious pages.
- Ensure that decision-makers responsible for network security and the brand are available 24x7.

- Create e-mail aliases with names such as “abuse,” “phishing,” and/or “fraud” at the company’s e-mail address—for example: fraud@YourCompanyName.com.
 - Encourage customers, vendors, and partners to report any suspected attacks or abuses of the company name or brand.
 - Monitor aliases 7 x 24, 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.
- Local, state and federal laws may influence both an organization’s response and which parties can help it. The laws are convoluted, so the organization’s incident response team should be aware of the local legal situation, as well as resources that are available to assist the team.
- Review the company’s insurance policy for coverage on losses due to phishing attacks and business continuity coverage.

Responding to Incidents

According to APWG data 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. (As stated previously, however, if ICANN changes its policy on releasing a domain owner’s name, contacting the owner could become more difficult.) With phishing sites, it is often the case that the original registrations 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 and or 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 through 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/or close their account.
 - Considering placing a "fraud alert" on your organization's home page and online login screens to alert visitors to the threats and where to go for assistance or more information.
 - Give customer service details of the attack so they can reassure customers reporting 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 references to images on the phishing site that actually reside on its site—and then mark those image files on its domain as "fake" or "phishing." That way, when those images appear on the phishing site the tags will alert the visitor.
 - Identify where phished information is being sent. It can then 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, it should submit its data to the Anti-Phishing Working Group (APWG) 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.
- Once the site has been rendered inoperative, try to purchase 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:

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 may be reproduced and distributed free of charge to an organizations employees and customers. Find them at www.microsoft.com/security.

Information and resources for IT Professionals and business may be found at www.microsoft.com/safety

- Educate employees and customers on 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 what domain names it owns, as well as 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 its external-facing servers and client computer systems
- Deploy Sender ID to authenticate inbound and outbound e-mail
- Deploy the Microsoft Phishing Filter through Microsoft Internet Explorer 7
- 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, and RSA Security

While none of these efforts are 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.

Anti-Phishing Working Group (APWG)	www.antiphishing.org
Authentication and Online Trust Alliance (AOTA)	www.aotalliance.org
Direct Marketing Association (DMA)	www.the-dma.org
E-mail Sender and Provider Coalition (ESPC)	www.espccoalition.org
Federal Trade Commission (FTC)	www.ftc.gov
Internet Corporation for Assigned Names (ICANN)	www.icann.org
Internet Crime Complaint Center	www.ic3.gov
Messaging Anti-Abuse Working Group (MAAWG)	www.maawg.org
Microsoft Safety technologies	www.microsoft.com/safety
Sender ID Framework	www.microsoft.com/senderid
TRUSTe	www.truste.org
U.S. Chamber of Commerce	www.uschamber.com/sb/security

Microsoft Safety and Security Downloads

Microsoft security resources	www.microsoft.com/security
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, we will update this white paper at www.microsoft.com/safety in "Technology Focus" or www.uschamber.com/sb/security in "Cyber Security Advocacy."