



Protecting Your Brand, Customers and Employees from online Threats *Creating a Competitive Advantage*

**By Craig Spiezle
Director of Internet Security
Microsoft Corporation**

Unsolicited e-mail and deceptive web sites become an expensive and at times dangerous problem for users, organizations and companies who depend on e-mail and the internet to communicate and conduct ecommerce and online banking.

Upwards of 80% of email purporting to be from legitimate brands is forged, significantly impacting user trust and confidence as well as the value of the respective brand. These messages try to entice users to open virus-laden attachments, connect to phishing sites and to reveal personal or corporate data, continuing to impact user's privacy, as well as the ever increasing a threat to corporate data and systems infrastructure. Domains owned by leading online financial services, banking sites, auction sites, travel sites, retailers and other sites that conduct Internet transactions are increasingly being targeted by these online criminals.

Technology solutions must include multiple lines of defense, including prevention, detection and remediation, providing users with a higher level of assurance of legitimate websites, and detection of deceptive email. Many leading industry solutions including Windows Internet Explorer 7, Exchange 2007 and Windows Live Hotmail offer integrated and dynamic prevention. Leading examples include email authentication via Sender ID and integrated browser protection including dynamic phishing detection and support for Extended Validation (EV) SSL certificates.

Email Authentication, The First Line of Defense

Sender ID Framework (SIDF) is a leading email authentication protocol offering simple and cost effective approach to fighting spam and phishing by detecting e-mail forgery. Sender ID authenticates inbound e-mail to verify it is from the domain it says it is from. Validating the IP address of the server sending the email via a DNS entry for the domain owner, ISPs and anti-spam solutions consider the Sender ID authentication result when determining if a message gets delivered, blocked or quarantined. Today nearly 50% of all legitimate email is authenticated and Sender ID compliant; supported by over 15 million domains worldwide. Organizations and marketers who have adopted Sender ID, and have a positive reputation, realize increased deliverability with up to 85 percent fewer messages mistakenly marked as spam and an increased spam and phishing detection. Sender ID is available industry-wide including Windows Live Hotmail and Exchange Server. Complementing SIDF, a second and emerging standard, is Domain Keys Identified Email (DKIM). Combined, both solutions provide comprehensive protection and interactive marketers and domain owners should consider implementing both protocols to maximize protection of their brand and customers. www.microsoft.com/senderid

Microsoft Phishing Filter

The Microsoft® Phishing Filter, a powerful security innovation in dynamically protecting consumers and businesses against fraudulent websites and data theft. Today this technology blocks nearly 1 million attempts to visit confirmed phishing sites weekly ; protecting over 200 million users of Windows® Internet Explorer® 7, for Microsoft Windows® XP Service Pack 2 and Windows Vista™ .

The Microsoft Phishing Filter is an opt-in service that operates in the background and provides an early warning system to notify users of both suspicious websites that could be engaging in identity and data theft, as well as those confirmed to be phishing sites. By design, user privacy has been at the forefront of this service and verified by third party audits that no personal information is transmitted or collected by Microsoft or any third party.¹ It relies on browser-based heuristics to analyze Web pages in real time and warn users about suspicious characteristics as they browse. This client-side technology is combined with dynamically updated information that helps prevent users from interacting with confirmed phishing sites reported to Microsoft by a network of third-party data-provider partners and a community of users who help provide information on potential and confirmed phishing sites.

Microsoft works with a growing list of commercial data providers to deliver rapid updates to the Microsoft Phishing Filter service who directly upload their data on confirmed Phishing sites to Microsoft, which aggregates these uploads and dynamically refreshes the database. Sharing your data with these providers can help augment your brand protection efforts.

<http://www.microsoft.com/safety/antiphishing>

Extended Validation (EV) SSL Certificates

Historically website security has focused on protecting information in transit—helping to keep information safe from prying eyes. While it protected your information from being accessed by 3rd parties, the solution didn't give you any information about the owner of the website or consistent validation of the business making the request. Phishers have taken advantage of this and have been able to obtain 'valid' SSL certificates for their bogus sites. Some phishing sites have secured commonly misspelled domain names so users are less likely to notice the extra character in the address bar. Looking for that gold padlock icon is important, but without the identity information users can end up sending your personal information to the wrong website.

Responding to these threats, the CA/ Browser Forum has developed the Extended Validation (EV) SSL Certificate, now adopted by over 4,000 web sites.² EV certificates help increase online safety and security by consistently taking several extra steps to validate the business entity in addition to the

¹ Third Party audit performed by Jefferson Wells. More information is available at www.microsoft.com/safety/antiphishing

² Source: Netcraft – November 2007

certificate request. This comprehensive review not only helps to avoid issuing certificates 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. Internet Explorer 7 displays 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.

EV SSL certificates are particularly useful for companies who may be at risk of being targeted by phishing schemes and other types of Internet fraud and desire to enhance level of user trust and confidence with their brand. Early adopters include the likes of Alaska Airlines, Charles Schwab, eBay & Paypal and British Airlines. <http://www.microsoft.com/windows/products/winfamily/ie/ev/default.msp>

Summary

There is no silver bullet or single solution to stop or combat spam, phishing and online deception — it takes a combination of innovative technologies, user education, enforcement, and collaboration. The Sender ID Framework, Microsoft internet Explorer 7, Microsoft Phishing Filter and EV SSL Certificates are examples of simple yet innovative, cost effective and easy-to-deploy solutions, developed in collaboration with industry partners and organizations throughout the world.

Improving online trust and confidence requires industry wide support. Leading organizations committed to improving online safety include the Anti-Spyware Coalition, Authentication and Online Trust Alliance (AOTA), Anti-Phishing Working Group (APWG), CA Forum, Experience Email Council (EEC), ESPC, TRUSTe and others.

Businesses have an opportunity and a responsibility to adopt these measures to protect their customers, brand, employees and stockholders. Early adopters will receive a competitive advantage in supporting the trust ecosystem.

For more information on Microsoft's holistic efforts and online safety technologies, visit www.microsoft.com/safety

Leading Organizations Committed to Online Safety & Collaboration

For additional listings visit <http://www.microsoft.com/mscorp/safety/industry/alliances.msp>

Anti-Phishing Working Group (APWG) - <http://www.antiphishing.org/>

The Anti-Phishing Working Group (APWG) is a global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.

Authentication & Online Trust Alliance (AOTA) - www.aotalliance.org

Founded in October 2004, the mission of the Authentication and Online Trust Alliance (AOTA) is to foster the elimination of email and Internet fraud, abuse and data intrusions thereby enhancing online trust, confidence and online protection of businesses and consumers. AOTA's goals are to spur the development of a "trust ecosystem" working with leading business, brands, industry and non-profit organizations, enhancing confidence, safety and privacy in email and ecommerce.

CA/Browser Forum - www.cabforum.org/forum.html .

The Certification Authority Browser Forum (CA/Browser Forum) is comprised of leading certification authorities (CAs) and vendors of Internet browser software and other applications. Members of the CA/Browser Forum have worked closely together in defining the guidelines and means of implementation for the Extended Validation (EV) SSL Certificate standard as a way of providing a heightened security for Internet transactions and creating a more intuitive method of displaying secure sites to Internet users. Information is available at

Experience Email Council (EEC) - <http://www.emailexperience.org>

The eec is a global professional organization that strives to enhance the image of email marketing and communications, while celebrating and actively advocating its critical importance in business, and its ROI value. We are committed to regularly conducting a broad series of email initiatives for a variety of organizations that highlight the positive impact and importance of email as a marketing tool, communications vehicle and branding device.

Email Sender & Provider Coalition (ESPC) - <http://espcoalition.org>

The Email Sender and Provider Coalition is a cooperative group of industry leaders working to create solutions to the continued proliferation of spam and the emerging problem of deliverability. The ESPC is currently working on solutions to spam and deliverability concerns through a combination of legislative advocacy, technological development, and industry standards.

Messaging Anti-Abuse Working Group (MAAWG) - <http://www.maawg.org>

MAAWG is a global organization whose goal is to enhance user trust and confidence by protecting electronic messaging from online exploits and abuse, while ensuring the deliverability of legitimate messages. With a broad base of Internet Service Providers (ISPs) and network operators, representing over 600 million mailboxes, MAAWG works to address messaging abuse by focusing on technology, industry collaboration, and public policy initiatives.