

# Achieving a Global Internet

At Microsoft, we are committed to promoting a safe online experience to help empower individuals and organizations worldwide to confidently rely upon the Internet to interact, to communicate, and to conduct business.

We believe achieving that goal requires a coordinated approach that includes innovative technology solutions, industry collaboration, prescriptive advice, education and user enablement, effective legislation, and targeted enforcement. Through our industry, business, and government partnerships, we are working to improve online safety and user confidence and to put the spammers, phishers, and scammers out of business.

**The security of Microsoft's customers is a top priority for the company.**

Today's interconnected world, with affordable and powerful PCs, high-speed connectivity, and an explosion of mobile devices, has created extraordinary new possibilities for computer users. It facilitates rich online experiences for end users around e-commerce, communications and entertainment. It gives businesses worldwide the opportunity to accelerate revenue growth and drive productivity gains, via scenarios ranging from e-commerce to online collaboration with partners.

Security needs to be a key enabler for these scenarios. As part of the Trustworthy Computing Initiative launched more than three years ago, Microsoft Corp. has made security as a top companywide priority.

**Microsoft's security vision is to establish trust in computing to realize the full potential of an interconnected world.**

To achieve this vision, Microsoft is taking a holistic approach toward security. The strategy is to provide a secure platform strengthened by security products, services and guidance to help keep customers safe. The company's

efforts focus around three key areas: technology investments, prescriptive guidance and industry leadership.

### ***Legislation and Public Policy***

Technology, enforcement, and industry collaboration efforts need to be supported by effective public policy, strong legislation that prohibits deception, empowers consumers, and protects e-commerce. We are joining with partners worldwide in these efforts.

- ***Technology Investments***

Microsoft is making investments to achieve the highest level of quality in Microsoft® software, and to deliver security technology innovations in the platform, security products and hosted security services.

- ***Prescriptive Guidance***

Microsoft is investing in providing educational resources, training, supportive tools and global outreach to help customers secure their environments and comply with regulations. Further information can be found at <http://www.microsoft.com/security/guidance>.

- ***Industry Leadership***

Microsoft is working with governments, industry partners, law enforcement agencies and others to address the key societal challenges of security, including spam, security, privacy and children's online safety. Further information can be found at <http://www.microsoft.com/mscorp/safety/industry/default.aspx>.

Security needs to be a key enabler in allowing customers to realize the potential of an interconnected world. End users and corporations need to know that their IT infrastructure is safe and secure. They need to be protected from all kinds of malware attacks, need to ensure that only legitimate users have access to their systems, applications and data, and that they comply with the ever-increasing set of regulations. They need tools and guidance to manage across the entire security life cycle — policy (“where do I want to be?”), assessment (“where am I now?”), remediation (“make it so”) and monitoring (“keep it so”).

---

The fundamental goals of information security are widely accepted as helping ensure information confidentiality, integrity, availability and accountability. Confidentiality involves controlling who gets access to information and resources. Integrity implies providing control of how information changes or resources are used. Availability entails timely access to information and resources while accountability is knowing who has access to information and resources.

### ***Providing Customers a Safe and Secure Online Experience***

As part of Microsoft's overall online safety strategy, Microsoft is strongly committed to working with industry, government, and law enforcement agencies to help improve online safety, trust, and confidence in the Internet and in all forms of electronic messaging.

Because cyber crime crosses jurisdictional boundaries, Microsoft works with governments and NGOs worldwide to enact legislation that prohibits the distribution of deceptive e-mail or spyware, protects individual privacy, empowers consumers, and preserves the health and vitality of legitimate e-commerce. To be effective, these laws need to follow consistent worldwide standards, contain proportionate and deterrent penalties—including statutory damages and recovery of profits—and foster cooperation among enforcement agencies.

We are seeing progress: numerous legislative bodies around the world have adopted cyber crime laws to address the worldwide proliferation of spam, phishing, malicious code, and spyware attacks. The United States, for example, has complementary federal and state cyber crime laws, which are helping to curtail cyber crime. The federal CAN-SPAM Act of 2003 empowers the FTC, state attorneys general, and Internet service providers to take strong action against deceptive spammers and phishers.

### ***Enforcing the Laws***

Microsoft works closely with law enforcement agencies around the world to take action against cyber criminals. These enforcement actions target the

worst offenders while aiming to deter others. Since 2003, Microsoft has supported hundreds of legal actions against spammers, phishers, and other cyber criminals worldwide, including filing 110 civil lawsuits against spammers and 129 civil lawsuits against phishers in the United States. In addition to these private actions, Microsoft has also collaborated with the Federal Trade Commission (FTC) and attorneys general in California, Florida, Massachusetts, Texas, and Washington State to investigate and pursue cyber criminals.

In March 2006, Microsoft announced the **Global Phishing Enforcement Initiative (GPEI)**, a worldwide consumer-protection campaign in which industry and law enforcement join forces to fight the phishers. The GPEI's activities address three key areas:

- Protection from fraudulent sites
- Partnerships with law enforcement and industry
- Prosecution of enforcement cases through worldwide investigative support

#### Recent Successes in the Fight Against Cyber Crime

On January 24, 2006, Microsoft joined with the Washington State Attorney General in filing parallel anti-spyware lawsuits—the state's first legal action under the Washington Computer Spyware Act, which was enacted in 2005. Microsoft filed its own lawsuit alleging violation of the same law.

In January, 2006, Bulgarian law enforcement arrested eight people who were suspects in an international criminal network responsible for financial fraud and stealing personal data via the Internet. Microsoft provided information to Bulgarian law enforcement that helped in the investigation and subsequent identification of the alleged perpetrators.

On August 9, 2005, Microsoft announced that it had reached a \$7 million settlement against former self-proclaimed "Spam King" Scott Richter and his

Colorado-based company OptInRealBig.com, LLC. Microsoft commenced the lawsuit against Richter on December 18, 2003, in conjunction with a parallel action by the New York Office of the Attorney General.

In August 2005, Microsoft provided investigative and technical support to U.S. and foreign law enforcement agencies that led to the arrest of the individuals suspected of authoring and distributing the MyTob and Zotob worms. Turkish and Moroccan law enforcement agencies made the arrests less than two weeks after the worms were unleashed.

### ***Collaboration with Industry and Law Enforcement***

Microsoft collaborates with law enforcement around the world to support cyber crime prosecutions and to promote safety for all users of the Internet, particularly children. For example, Microsoft worked closely with Canadian police and international law enforcement to develop the [Child Exploitation Tracking System \(CETS\)](#), a unique software tool that provides investigators with software to store, search, share, and analyze large volumes of evidence and match cases across police agencies.

In April 2004, Microsoft joined with Interpol and the [International Centre for Missing and Exploited Children \(ICMEC\)](#) to announce the launch of the Global Campaign Against Child Pornography. In conjunction with this campaign, Microsoft has helped the ICMEC and Interpol sponsor worldwide training sessions for law enforcement personnel on the subject of computer-facilitated crimes against children. As of June 2006, the sessions had trained more than 1,500 officers from nearly 90 countries on methods for identifying suspects, investigating offenses, and dealing with victims of online child abuse.

Microsoft is a founding member of [Digital PhishNet \(DPN\)](#), a collaborative enforcement operation that unites industry leaders in technology, banking, financial services, and online auctioneering with law enforcement to tackle phishing. DPN connects private industry with such law enforcement agencies as the Department of Homeland Security, Federal Bureau of Investigation (FBI), and the U.S. Secret Service.

### ***Education and Awareness: Helping Customers Protect Themselves Online***

The Internet and e-mail are vibrant resources, powerful tools, and a critical part of the world's communications and business infrastructure. They are also under constant attack. The spam, phishing, and online threats have evolved from an annoyance into a threat that challenges the viability of electronic communications for users worldwide. Most spam contains misleading information designed to generate an online purchase or, worse, to trick recipients into disclosing sensitive personal information or confidential corporate data or downloading malicious software. At Microsoft, we believe we must not only deliver strong technology to address online problems, but also provide information and resources to empower individuals and organizations to better understand how they can help protect themselves.

### ***Helping Users Know Where to Start***

Nothing can guarantee complete safety in cyberspace, but much can be done to help users understand and minimize their exposure to risk. We make available a wide range of resources to help users protect their businesses, their computers, and their personal information. Instructions, advice, tools, and videos are available from both [Microsoft.com Security](http://Microsoft.com/Security) and [www.staysafe.org](http://www.staysafe.org). Both of these Web sites provide prescriptive guidance to help protect children online, combat online fraud, reduce spam, avoid phishing scams, and preserve privacy. Other sites, such as the Federal Trade Commission's [www.onguardonline.org](http://www.onguardonline.org), the Internet Education Foundation's [www.getnetwise.org](http://www.getnetwise.org), and the National Cyber Security Alliance's [www.staysafeonline.org](http://www.staysafeonline.org) also provides advice to consumers.

### ***Protecting Consumers Requires an Industry-wide Approach***

Leading e-mail infrastructure and services providers share the same challenges with spam, phishing, and identity theft as users do. Any solution to the problem of spam and phishing must involve coordinated industry efforts on many levels throughout the Internet and e-mail ecosystem. At Microsoft, we are working with key stakeholders such as America Online, Amazon, Bell Canada, British Telecom, Cisco, Comcast, eBay, Sendmail,

Symantec, and Yahoo! to help drive technical collaboration and to develop effective industry guidelines and best practices to address these problems.

### [Industry Working Groups, Organizations, and Alliances](#)

At Microsoft, we work closely with various industry organizations and trade associations to share information and coordinate efforts toward common goals. Through supporting and serving in leadership roles with these organizations, we can jointly improve online trust and confidence.

### [Reputation Services](#)

Reputation services play a critical role in e-mail authentication and identity verification. Microsoft works closely with several companies that provide such reputation services to improve the deliverability of legitimate e-mail and reduce false positives.

### [Microsoft Phishing Filter Data Providers](#)

To provide an unparalleled level of protection from phishing exploits, Microsoft has agreements with several commercial data providers to dynamically provide information to Microsoft on thousands of confirmed phishing Web sites. Microsoft has integrated this data into the new Microsoft Phishing Filter technology, which is available for the MSN Search Toolbar and the preview betas of Internet Explorer 7 for Microsoft Windows Vista and Microsoft Windows XP SP2. Today this data is helping to improve online safety for millions of users worldwide.

### [Sender ID Support and Solutions](#)

Many companies offer technical solutions that support the Sender ID Framework. These solutions can help you combat spam and phishing today.

## **Conclusion**

Microsoft is committed to delivering software, services and best practices that together will help protect customers' systems so they can fully leverage the benefits of technology and the Internet with the confidence that their systems are protected.

To achieve this, Microsoft's security and Internet safety efforts are focused in three primary areas:

1) Technology Investments: to improve the security of its products, improve the update process, and provide new features and products that improve safety;

2) Industry Partnerships: with partners, customers, governments and law enforcement agencies to assist the development of policies and actions that can be enforced against cyber criminals;

3) Prescriptive Guidance & Education: broadly distributed, timely information to help make customers their systems more secure and prepare against emerging threats.

Microsoft recognizes security is a long-term journey, but through new security innovations like Windows XP Service Pack 2, Windows Server Service Pack 1, improvements in the quality and predictability of product updates, broadly available security guidance and collaboration with customers, partners and governments — Microsoft has taken the first steps to help consumers and businesses protect themselves.