Microsoft

Online Safety

Building Global Trust Online, 4th Edition

Microsoft Perspectives for Policymakers

Contents

Online Safety at Microsoft: Building a Safer Digital World

Microsoft supports digital citizenship—safer, responsible, and more appropriate use of technology and devices.

What is online safety?

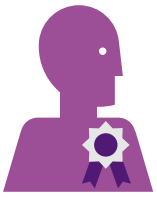
Online safety is the practice of maximizing desirable digital experiences and minimizing those tied to illegal, inappropriate, or illegitimate content, contact, conduct, or commerce –"The 4 Cs."

CONTENT

Users can be exposed to inaccurate, inappropriate, or objectionable content online.

CONTACT

Interactions online can lead to unwanted contact.



CONDUCT

How we act online affects our own reputation as well as others.

COMMERCE

Criminals attempt to steal sensitive personal information and money by breaking into business databases and personal accounts or through scam solicitations.

The Microsoft approach to online safety

Microsoft defines the discipline of online safety in terms of risk management. To help people minimize their risk online, Microsoft:

DEVELOPS TECHNOLOGY TOOLS

Microsoft offers a range of technologies for online safety.

MICROSOFT SECURITY ESSENTIALS

INPRIVATE BROWSING

SMARTSCREEN FILTER

BING SAFESEARCH

MICROSOFT FAMILY SAFETY TOOLS

REPORT ABUSE MECHANISMS

PROVIDES EDUCATION AND GUIDANCE

Microsoft puts its passion for online safety into practice by:

Offering guidance on how people can better secure their devices and help protect their information and families online through the Microsoft Safety & Security Center.

Conducting research, like the Microsoft Computing Safety Index, to gauge online safety behaviors and improve digital lifestyles.

ESTABLISHES PARTNERSHIPS

Everyone plays a role in helping to create a safer and better Internet.

PARENTS AND CAREGIVERS

EDUCATORS

TECHNOLOGY INDUSTRY

LAW ENFORCEMENT AND GOVERNMENT

NONGOVERNMENTAL ORGANIZATIONS

Read on to learn more about online safety at Microsoft

Online Safety

Key Points

- The Internet enriches lives in many ways, but it also presents risks to privacy, safety, personal and professional reputations, and commerce due in part to the online presence of cybercriminals and malicious software.
- Microsoft defines the discipline of online safety in terms of risk management. To help people minimize their risk online and to create safer, more trusted computing experiences, Microsoft develops technology tools; provides education and guidance; and partners with government, industry, law enforcement, and nonprofit organizations.
- Online safety is a shared responsibility, and government and industry must work together to support it.

The Internet has revolutionized the way we work, learn, communicate, and play. However, it has also created new risks and potential for harm. These include infection of devices by malicious software, such as viruses; victimization by online scammers selling counterfeit goods or pushing fraudulent investment schemes; loss of privacy; and identity theft by criminals.

Many people are concerned about these risks, but they often fall short in taking the steps necessary to protect themselves. Since 2011, the Trustworthy Computing group at Microsoft has sponsored the Microsoft Computing Safety Index (MCSI), an annual study that measures the actions that consumers take to help keep themselves and their families safe online. The 2013 MCSI sampled 10,500 adults in 20 countries and regions worldwide. Results showed that although users are cautious (for example, conducting transactions on reputable websites and using strong passwords), they often miss taking active steps to keep themselves safer, such as locking mobile phones or adjusting privacy settings on social sites.

Addressing the challenges of online safety requires collaboration between the technology industry and government. Technology companies must commit to protecting sensitive data and personal information as well as facilitating business practices that promote trust. Governments can support industry self-regulation and legislative frameworks that foster an environment of technological innovation.

Microsoft Approach

Grounded in its Trustworthy Computing initiative, Microsoft has a longstanding commitment to online safety, which the company's Chief Online Safety Officer oversees. The Chief Online Safety Officer is responsible for all aspects of Microsoft online safety strategy, which includes creating and implementing internal policy, influencing the development of safety features and functionality in Microsoft products and services, and engaging with an array of external audiences. Microsoft defines the discipline of online safety in terms of risk management. The company views its role as helping people maximize desirable online experiences while minimizing the risks by:

DEVELOPING TECHNOLOGY TOOLS

- Microsoft Security Essentials, a free antimalware program, is available for download.
- Microsoft account holders can specify who may view their profiles, who can contact them, and who can post or view the content they share. Internet Explorer also helps manage people's privacy with InPrivate browsing and the SmartScreen Filter that helps warn users about phishing sites.
- Microsoft offers family safety tools to help protect children online in all editions of Windows 7 and 8, on Windows Phone, and in Xbox products and services. Bing provides the SafeSearch feature, which can help keep adult content out of kids' search results.

PROVIDING EDUCATION AND GUIDANCE

- The Microsoft Safety & Security Center offers tips and advice on how people can better secure their devices, protect their reputations and families online, and evade online scams.

- The Microsoft Safer Online team raises public awareness about online safety habits and practices through its participation in such events as Safer Internet Day and National Cybersecurity Awareness Month, as well as presentations at the Internet Governance Forum

PARTNERING WITH OTHERS

- Microsoft works with nongovernmental organizations, law enforcement, and other technology companies on online safety issues. The company collaborates with organizations like the Family Online Safety Institute (FOSI) and the National Cyber Security Alliance (NCSA).

- Microsoft developed and shared PhotoDNA, a technology that helps nongovernmental organizations, law enforcement, and other technology companies find and remove from the Internet some of the worst images of child sexual abuse.

- The company offers technical training to law enforcement agencies and develops new tools to help them combat cybercrime. Microsoft also works with law enforcement to stop cybercriminals through legal action, including steps to take down botnets and shut down the purveyors of fake security software.

Policy Considerations

SUPPORT INNOVATION AND SELF-REGULATION As governments address the risks associated with emerging technologies and online services, it is important that they support industry self-regulation and legislative frameworks that foster an environment of technological innovation.

ENCOURAGE PUBLIC-PRIVATE PARTNERSHIPS Government and industry can work together to establish safety principles and help service providers fulfill their safety promises. Examples include ISP codes of practice in Australia (and other countries) to help secure a fair and open Internet,[1] recommendations from the EU CEO Coalition[2] to make the Internet a safer place for children, and the UK Search Engine agreement to block illegal search terms and images of child sexual abuse.[3]

SUPPORT RESEARCH THROUGH COMMISSIONS AND FUNDING Research plays a critical role in identifying factors that increase online risk and in dispelling myths that can lead to misplaced efforts to address them. Government commissions and funding to advance Internet safety are essential to support both academic and industry research.

PROMOTE ONLINE SAFETY EFFORTS IN EDUCATION Online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should weave into the standard curricula modules that focus on digital literacy and civility.

---

1 *Internet Industry Code of Practice Version 6:* iia.net.au/codes-of-practice/internet-industry-code-practice-version-6.html
2 *Self-Regulation for a Better Internet for Kids:* aka.ms/EC-SaferInternet
3 www.gov.uk/government/news/internet-safety-summit-at-downing-street-communique

Digital Citizenship

Key Points

- The Internet presents great opportunities, but it is not without real risk of experiencing inappropriate content, contact, conduct, or commerce. The risks can be mitigated by teaching digital literacy and civility—elements that are central to good digital citizenship.

- Microsoft created the Digital Citizenship in Action Toolkit expressly to teach young people and adults how to become good digital citizens, and the company promotes digital literacy programs in 134 countries.

- Education policymakers should broaden online safety efforts and adopt a set of national goals for online safety, including minimum standards for digital literacy curricula.

New information technologies have profoundly changed the world—the immense resources of the Internet and the accompanying array of Internet-enabled devices and services give everyone tremendous opportunities to work, learn, communicate, and play. While largely positive, the Internet has also created new potentials for harm. These include infection by malicious software, such as viruses, worms, and spyware; victimization by online scammers selling counterfeit goods or pushing fraudulent investment schemes; loss of privacy and damage to online reputation; and identity theft by criminals.

Governments, the technology industry, and public sector organizations have addressed this risk to online safety through technology tools, policies, law enforcement activities, and education. These approaches play important roles, but to be successful, strategies (educational approaches in particular) must take into account the social norms and behaviors that everyone, including young people, must understand to become responsible digital citizens.

The concepts of digital citizenship—the safer, more responsible, and appropriate use of technology and devices—underpin such an approach. In becoming good digital citizens, people develop a sense of ownership and personal responsibility that will help them make ethical decisions in the online world, and in so doing build a safer, more trusted Internet. Digital citizenship is grounded in two primary elements: digital literacy and civility.

DIGITAL LITERACY Those who are literate in the online world are better prepared to avoid risky situations, make better-informed decisions, and better understand how to protect their privacy. They have learned such basic online safety habits as how to protect their accounts and reputation, the importance of strong and secret passwords, and how to update their computers and devices to defend against malware and scams. Digital literacy also requires the critical thinking skills needed to evaluate online information and situations and to problem-solve.

DIGITAL CIVILITY Digital literacy provides a solid foundation for digital citizenship, but Internet users must also demonstrate respect for others—behaving with civility and being protective of everyone's rights (their own included). People must learn and apply the skills to behave ethically and within online social norms. These skills include being judicious about what they say and do online; protecting others' privacy by not sharing personal details of friends and family without their permission; and respecting the intellectual property of others—for example, downloading only legal copies of copyrighted material.

Microsoft Approach

MATERIALS TO TEACH DIGITAL CITIZENSHIP The Digital Citizenship in Action Toolkit was created expressly to teach people how to become good digital citizens. Fact sheets, tip cards, videos, and other materials give information about safer social networking, inappropriate behavior (like online bullying), using mobile devices more safely, responsible online gaming, and protecting oneself from online fraud and identity theft.

WORLDWIDE SAFETY EDUCATION PROGRAMS Microsoft promotes digital literacy programs in 134 countries with a particular focus on broadening the reach beyond those who speak English and other commonly used languages. Programs include Partners in Learning and YouthSpark.

SUPPORT FOR ONLINE SAFETY CURRICULA IN SCHOOLS Microsoft believes that digital citizenship is an important component of any school curriculum; it supports the integration of digital citizenship concepts in technology instruction for students, with key topics woven into existing curricula.

Policy Considerations

Policymakers in government and industry can help companies work more securely on the Internet and protect company data and financial assets against cybercrime by adhering to the following principles:

- **EMPHASIZE DIGITAL CITIZENSHIP EDUCATION** Education policymakers should broaden online safety efforts to include an emphasis on digital citizenship through digital media literacy and education programs. They should also adopt a set of national goals for online safety, including minimum standards for digital literacy curricula.

- **SUPPORT FUNDING OF DIGITAL CITIZENSHIP PROGRAMS** Governments should ensure that all digital literacy and online safety programs are funded through competitive grants open to qualified applicants, with periodic review and assessment built in so that the results from the best programs can be replicated in other communities.

- **PROVIDE LEGISLATION SUPPORTING DIGITAL SAFETY CURRICULA** Some jurisdictions require that online safety education be an integral part of school system efforts to achieve digital literacy for their students. Legislation requiring schools to implement online safety education should be broad enough to account for local variations in curricula. One example is a US law mandating that Internet safety be included in the curricula of any school that receives E-Rate funding[4] from the Federal Communications Commission (FCC), which gives schools and libraries discounts for telecommunications and Internet access.

- **PROMOTE INDUSTRY SELF-REGULATION AND INNOVATION** As governments address the risks associated with emerging technologies and online services, it is important that they support industry self-regulation and legislative frameworks that encourage technological innovation.

---

4 *Laws Require Internet Safety Education in Schools that Receive E-Rate Funds:* aka.ms/E-Rate_online_safety_educ

Child Online Safety

Key Points

- Although the Internet enables many enriching experiences for children, there are also risks, including potential exposure to inappropriate content, contact with bullies, and loss of privacy.
- The Microsoft approach to children's online safety includes creating innovative technology tools; providing education and guidance; establishing robust internal policies and practices for moderating content and addressing online abuses; and partnering with nongovernmental organizations, industry, law enforcement, and others.
- The safety of children online is a community challenge and government, industry, and others should work together to establish and implement safety principles. As governments address risks associated with emerging technologies and online services, it is important that they continue to encourage innovation and technology adoption.

Although the Internet offers a wealth of positive experiences for children, parents face challenges when monitoring the content their children encounter online, the people they meet there, and what they share.

INAPPROPRIATE CONTENT

Young people are curious and may stumble upon inappropriate material (including hateful or sexual content) by clicking a link in email, on a social network, or while searching for something else on the web.

INAPPROPRIATE CONDUCT

Young people—and adults, too—may use the Internet to harass or exploit others. Kids may sometimes broadcast hurtful bullying comments or embarrassing images. A particular concern with mobile devices is sexting—the transmission of sexually explicit photographs and videos taken with a device's camera.

INAPPROPRIATE CONTACT

Adults—and young people, too—use the Internet to find and approach vulnerable youth. Frequently, their goal is to develop what youth believe to be meaningful online relationships, a process referred to as *grooming*.

INAPPROPRIATE COMMERCE

Children can easily fall victim to phishing or other scams. They can be enticed to click a flashy ad, open an appealing "free" game, or download a ringtone. These can install viruses, spyware, or other malicious software.

Microsoft Approach

The Microsoft approach to combating child safety issues on the Internet includes developing technology, providing education and guidance, establishing internal policies, and partnering with others.

CREATING TECHNOLOGY TOOLS Microsoft builds safety features into a wide range of its products and services to help parents minimize online risks to their children.

In all editions of the Windows 7 and Windows 8 operating systems, parents can use the Family Safety feature to create a separate account, with specific activity limits, for each family member.

The Xbox platform is equipped with parental controls to help create a safer environment for all gamers. For example, on Xbox One, parents can use Family and Online Safety controls to set a maximum age, which maps to ratings systems like Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI).

Windows Phone offers two ways to manage young people's access to games and apps. Young people under age 18 who have their own Windows Phone sign in with a child's account. Parents set up My Family, add the young person, and then manage what kids can download from the Windows Phone Store. For younger ones, parents can use Kid's Corner to create a space on their phone where children can play games, use apps, and watch videos that parents have selected.

Bing SafeSearch can help keep adult content in text, images, and videos out of children's search results.

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center provides age-based advice for Internet use, and guidance on such issues as online bullying, safer social networking, mobile device safety, responsible online gaming, and how to avoid, block, and report inappropriate behavior.

ESTABLISHING INTERNAL POLICIES AND PRACTICES Microsoft promotes online safety through robust company-wide policies, standards, and procedures for its web products and services. It enforces policies inherent in its code of conduct for users of its online services, and it moderates content and interactions to address illegal activity, inappropriate material, and other abusive content or contact.

PARTNERING WITH OTHERS To help promote online safety for children and young people, Microsoft:

Collaborates with industries and organizations like the Family Online Safety Institute, which sponsored A Platform for Good to start a dialogue about what it means to participate responsibly in a digital world.

Developed and shared PhotoDNA, an image-matching technology that helps nongovernmental organizations, law enforcement, and other technology companies such as Facebook and NetClean find and remove some of the worst images of child sexual abuse from the Internet.

Policy Considerations

Governments and other policymakers can help promote recent efforts in child online safety by focusing on these priorities:

STRENGTHEN AND ENFORCE EXISTING CHILD PROTECTION LAWS Governments must strengthen and enforce laws against the possession and distribution of child sexual abuse images. Microsoft works with the International Center for Missing & Exploited Children (ICMEC), INTERPOL, and other organizations to support government efforts.

ENCOURAGE PUBLIC-PRIVATE COLLABORATION Government and industry must collaborate to establish safety principles and offer a more secure online environment for youth. Examples of this collaboration include recommendations from the EU CEO Coalition[5] to make the Internet a safer place for children, the UK search engine agreement to block images of child abuse,[6] and the digital citizenship principles published by the Australian Communications and Media Authority (ACMA).[7] As governments address risks associated with emerging technologies, they must avoid stifling innovation and technology adoption.

PROMOTE COMPREHENSIVE ONLINE SAFETY EDUCATION IN SCHOOLS Programs should include modules that weave digital literacy (including how to avoid online dangers and protect devices) and digital civility into the standard curricula. Legislation requiring schools to implement online safety education should be broad enough to accommodate local variations in curricula.

SUPPORT INTERNET SAFETY RESEARCH Research is particularly important for identifying factors that increase online risk and for dispelling myths that can lead to misplaced efforts to advance Internet safety. Government funding for both academic and industry research in these areas is essential.

5 *Self-Regulation for a Better Internet for Kids:* aka.ms/EC-SaferInternet
6 www.gov.uk/government/news/internet-safety-summit-at-downing-street-communique
7 www.cybersmart.gov.au/cybersmart-citizens.aspx

Online Safety Education

Key Points

- The Internet is an extraordinary tool for enabling young people to learn about and explore the world around them, but it may also expose them to certain risks, such as inappropriate content, contact, conduct, or commerce. Comprehensive online safety education is a crucial part of teaching young people to address these risks and build the skills of good digital citizenship.

- Microsoft offers age-based guidance to help teach young people about online safety, promotes digital literacy programs in 134 countries, and encourages its employees to get involved in online safety education.

- Microsoft supports comprehensive online safety education in schools, with key topics woven into the existing curriculum. Legislation requiring schools to implement online safety education should be broad enough to account for local variations in curricula.

The immense resources of the Internet and the accompanying array of Internet-enabled devices give young people tremendous opportunities to learn, share, and communicate. Online, however, youth may be exposed to certain risks. These may include potential exposure to inappropriate content (including sexually explicit or hateful websites), contact (from predators), conduct (such as bullying or inappropriate sharing), or commerce (like identity theft or pirated music and games).

Comprehensive and age-appropriate online safety education plays a vital role in helping young people learn about those risks and how to avoid them. They'll learn this best in the context of developing positive online behaviors, such as respect for intellectual property and adherence to basic codes of acceptable conduct. This is often referred to as digital citizenship, the norms of behavior in online society. Learning these norms prepares young people to be good digital citizens in technology-rich societies. It helps them develop a sense of ownership and personal responsibility that, in turn, will help them make appropriate, ethical decisions in the online world.

Ideally, given the vast array of diverse subject material that educators much teach every day, the principles of digital citizenship should be woven into the existing curricula.

DIGITAL LITERACY

Young people should learn basic online safety habits: how to protect their accounts and reputation; the importance of strong and secret passwords; and how to update their computers and devices to defend against viruses, spam, and phishing scams. Digital literacy involves more than just technical competency—it requires critical thinking skills to evaluate different sources of information and situations, to solve problems as they arise, and to know when to report problems to the appropriate adults.

DIGITAL CIVILITY

Young people should learn the risks of bullying, plagiarism, and piracy, and learn the skills to behave ethically and operate within online social norms. These skills include standing up for friends, not sharing personal details of friends and family without their permission, downloading only legal copies of copyrighted material, and using social networks that are right for their age.

Microsoft Approach

The company makes contributions to online safety education that include the following:

The Microsoft Safety & Security Center provides age-based guidance—both online and in face-to-face training sessions and similar events—to help young people become good digital citizens with information about online bullying and inappropriate online behavior, safer social networking, safer use of mobile devices, and responsible online gaming.

Microsoft employees in 26 of its European subsidiaries reach more than 90,000 teachers, parents, and students. For example, in the United Kingdom and Australia, Microsoft employees developed a program called ThinkUKnow with local law enforcement officials to deliver online safety education and resources.

Microsoft promotes online safety and digital literacy programs in 134 countries, with a particular focus on broadening the reach beyond those who speak English and other commonly used languages. Activities include Partners in Learning, YouthSpark, the Unlimited Potential, and Community Technology Access programs.

Policy Considerations

Governments and other policymakers can help promote recent efforts in online safety education by focusing on these priorities:

- **SUPPORT ONLINE SAFETY EDUCATION EFFORTS IN PUBLIC SCHOOLS** A number of jurisdictions require that online safety education be an integral part of school system efforts to achieve digital literacy for their students, which is a trend that must continue and grow. For example, one US law mandates that anti-bullying measures be taught in any school that receives E-Rate funding from the Federal Communications Commission (FCC), which gives schools and libraries discounts for telecommunications and Internet access.[8]

- **SUPPORT TECHNOLOGY TRAINING FOR TEACHERS** Just as students need education about safer Internet use, teachers also need training to keep up with ever-changing technology. Teacher training for effective use of technology in the classroom must include an understanding of current Internet risks, recognition of when students may be subject to online dangers, and guidance for helping students conduct themselves with civility on the web.

- **BALANCE ONLINE RESTRICTIONS WITH SAFETY EDUCATION** Restricting children's Internet access may be appropriate in some areas, such as where age limits currently exist in the physical world—like gambling and pornography. But safety experts agree that restricting access is not enough and that education plays a vital role in the safety of young people online.

8 *Laws Require Internet Safety Education in Schools that Receive E-Rate Funds:* www.safeschools.info/bullying-prevention/bullying-prevention-news/362-laws-require-internet-safety-education-in-schools-that-receive-e-rate-funds

Family Safety Settings

Key Points

- Family safety settings help parents monitor their children's Internet use. Although they are not a substitute for parental involvement, family safety technologies can help reduce the risk of exposure of young people to inappropriate content, contact, conduct, and commerce.
- Microsoft has long provided the tools (including in Windows, Xbox, and Windows Phone) that parents need to help them put their decisions into practice in a way that supports their values and the maturity of their children.
- Decisions about what children can view online are best left to parents and caregivers, so Microsoft does not support efforts to require the use of parental controls or filtering software. Instead, governments must work with industry and nongovernmental organizations to help promote and publicize online safety technology.

Although the Internet offers many enriching opportunities for young people, there are also concerns about the content they encounter, the people they meet there, and what they share. One way to help protect youth is through technologies that parents and caregivers can use to monitor what children and teens are seeing, hearing, and doing online.

These family safety (or parental control) technologies—including content filters, contact management tools, and limits on the download and use of music, apps, and other files—have been used on personal computers since the early 1990s. Now, as mobile phones, tablets, and other devices have become Internet-enabled, technology companies have added family safety settings to them as well.

Family safety settings are widely used in many countries. In 2011, a survey in the United States by the Family Online Safety Institute (FOSI)[9] found that 54 percent of parents used them. Microsoft research in 2012 of 1,000 parents in Brazil, China, France, India, and the United States found that they were split between monitoring their children's online activity (43 percent) and limiting access (45 percent).

Despite their popularity and obvious utility, parental controls have generated controversy. Some have advocated that governments should mandate their use by minors; others have pushed for mandatory use by everyone, a position that human rights advocates and others strongly oppose; still others raised concerns about the misuse of such technology for spying by overzealous parents.

Microsoft Approach

Microsoft believes that the company's role in providing family safety tools is to help parents put their decisions into practice in a way that supports their values and the maturity of their children.

WINDOWS 7 AND WINDOWS 8 offer parents Family Safety, which they can use to create a separate account for each family member. Parents can then monitor where their children go and what they do online. For more control, parents can set daily time limits and block websites they specify.

WINDOWS PHONE offers two ways to manage the access of young people to games and apps:

- Young people under age 18 who have their own Windows Phone sign in with a child's account. They won't be able to download anything until parents set up My Family and add the young person. Once that's done, parents can manage the apps and games that their children can download from the Windows Phone Store.

9 Who Needs Parental Controls? A Survey of Awareness, Attitudes, and Use of Online Parental Controls: **www.fosi.org/research/900-who-needs-parental-controls.html**

- For younger ones, parents can use Kid's Corner to create a space on their phone where children can play games, use apps, and watch videos that parents have selected. While in Kid's Corner, the child can't purchase apps and won't be able to access functions that might not be age appropriate, such as web browsing or text messaging.

XBOX Microsoft was the first to produce a gaming console that introduced ratings-based parental controls.

- Xbox 360 Family Settings enable parents to set and enforce content ratings for games, movies, and television shows; they can also set limits on console play time using the family timer.

- On Xbox One, parents use Family and Online Safety controls to set a maximum age, which maps to ratings systems like Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI). Parents can then decide whether they want Xbox One to always block content that exceeds this rating or make that decision on a case-by-case basis.

- With Online Safety Settings for Xbox Live, parents can create individual profiles that are appropriate for each child's age and maturity. Parents can specify what activities children can participate in (such as multiplayer gaming, video chat, text messaging, or voice messaging), who they can communicate with, and who can see the child's profile or friends list.

Policy Considerations

Policymakers can help make technology and the Internet safer for families by promoting the following principles:

SUPPORT SELF-REGULATION INSTEAD OF MANDATORY COMPLIANCE Decisions about what children can view online are best left to parents and caregivers, so Microsoft does not support efforts to require the use of parental controls or filtering software. Instead, government must work with industry and nongovernmental organizations such as GetNetWise to help promote and publicize online safety technology.

ADDRESS RISKS IN EMERGING TECHNOLOGY WITHOUT STIFLING INNOVATION To better protect young people online, industry must regulate itself and government must develop thoughtful legislative frameworks for addressing risk in emerging technology areas. As governments do this, it is essential that they allow for innovation in the process.

PROMOTE SAFETY THROUGH COLLABORATION Government and industry must work together to establish safety principles that will help create a more secure online environment. Examples of this collaboration include the ISP codes of practice in Australia (and other countries) to help secure a fair and open Internet, recommendations from the EU CEO Coalition to make the Internet a better place for kids, and the UK Search Engine agreement to block illegal search terms, as well as images and video of child sexual abuse.

ENCOURAGE INTERNET INDUSTRY COOPERATION Policymakers should support legislation that releases access providers from liability for obscene material or abusive behavior if they have made a good-faith effort to screen their services or provided screening devices for parents. Examples include Section 230 of the US Communications Decency Act and the European Union Directive 2000/31/EC.

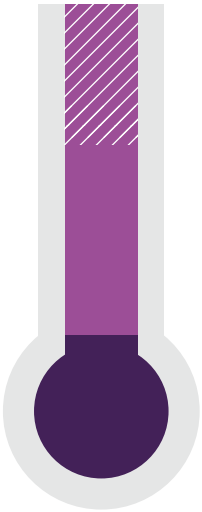
Microsoft Computing Safety Index

Key Points

- Microsoft uses the Microsoft Computing Safety Index (MCSI) annually to identify and rate the online security- and safety-related behaviors of people around the world. Microsoft's research, combined with the resulting Index, will help lead to safer technologies and programs for better educating web users.
- The Microsoft approach to online safety includes developing technology tools; providing education and guidance; and collaborating with industry, law enforcement, and nonprofit organizations.
- Policymakers can advance the impact of online safety by supporting and funding research to promote public awareness of online safety issues, as well as by encouraging innovation and self-regulation.

As more people connect online, the need for safety, security and privacy grows. Consumers are increasingly concerned about security breaches, fraud, and the collection and use of personal information. Microsoft believes that a better understanding of how people respond to and defend against these threats can help lead to safer technologies and better programs for educating web users.

Since 2011, Microsoft has fielded the Computing Safety Index, a survey that measures the steps people report taking to protect their computers, mobile phones, and information online. The survey organizes 24 protective steps into three categories. The more steps respondents report taking, the higher their Index score, with 100 being the highest rating.



- **BEHAVIORAL:** seven protective behaviors, from using unique passwords for each account or website to educating oneself about the most current ways to protect one's online reputation and defend against identity theft
- **TECHNICAL:** twelve technology tools that include using privacy settings, limiting what others can see on social sites, and locking mobile devices with a PIN or password
- **FOUNDATIONAL:** five basic protections like leaving the computer's firewall turned on and running automatic software updates

In May 2013, researchers surveyed more than 10,000 people age 18 and older in 20 countries and regions around the world.[10] They found that the steps people take to protect themselves online haven't changed much since the first survey.

When respondents checked their settings, researchers found that people scored relatively well on those foundational protections that are built into devices and software by technology companies.

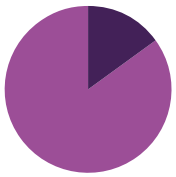
10 Australia, Belgium, Brazil, Canada, China, Egypt, France, Germany, India, Indonesia, Japan, Korea, Malaysia, Mexico, Russia, Singapore, Spain, Turkey, the United Kingdom, and the United States

However, by a large margin (60 percent), people see themselves as best able to protect their information rather than relying on technology companies, government, and others.

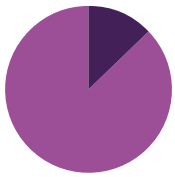
That doesn't seem to be the case.

- Only one in five (21 percent) of those surveyed took advantage of web browser filters that help protect against phishing.
- Just 31 percent educated themselves about the latest steps for protecting their online reputation or were selective about what they texted.·
- Only slightly more than one-third said they limit the amount of personal information that appears online (36 percent) or educate themselves about the most current ways to protect against identity theft (37 percent).

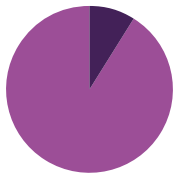
THE RESULT?



15% *of respondents said they or someone they know had been victims of a phishing attack*



13% *experienced damage to professional reputation*



9% *said their identity had been compromised*

Microsoft Approach

The Microsoft approach to online safety includes developing technology tools, providing education and guidance, and engaging through policy with governments and nonprofit organizations.

DEVELOPING TECHNOLOGY TOOLS Microsoft offers free technology tools to reduce online risk, including Microsoft Security Essentials, a free antimalware program. Internet Explorer offers settings to help people manage their privacy online, including InPrivate browsing, as well as the SmartScreen Filter that helps warn users about potential phishing websites. In addition, Microsoft has built family safety features into many of its products, including all editions of Windows 7 and 8 with Microsoft Family Safety (which helps monitor and protect children online), Windows Phone, and Xbox products and services.

PROVIDING EDUCATION AND GUIDANCE For decades, Microsoft has invested in consumer awareness about the safer use of technology and the Internet.

- The Microsoft Safety & Security Center offers online safety guidance to consumers. This includes tips for safer social networking, use of mobile devices, and online gaming, as well as guidelines for avoiding, blocking, and reporting inappropriate behavior.

- Microsoft has commissioned many studies in addition to the MCSI. These included surveys of parents and non-parents about kids' access to devices and online services, mobile phone manners and safety habits, as well as surveys of consumer concerns about online privacy and their personal information online.

ENGAGING THROUGH POLICY WITH GOVERNMENTS AND NONPROFIT ORGANIZATIONS Microsoft efforts have centered on engaging through public policy with governments around the world, as well as with nongovernmental organizations such as the National Cyber Security Alliance and the Family Online Safety Institute, and on such online safety initiatives as National Cyber Security Awareness Month, Safer Internet Day, and STOP. THINK. CONNECT.

Policy Considerations

Governments and policymakers can aid in fighting online security risks and help encourage safer online behavior by focusing on the following:

SUPPORT RESEARCH THROUGH COMMISSIONS AND FUNDING Research (like the MCSI) plays a critical role in identifying factors that increase online risk and in dispelling myths that can lead to misplaced efforts to address them. It is essential that government commissions and funding support Internet safety research.

PROMOTE PUBLIC AWARENESS OF ONLINE SAFETY Governments and technology companies worldwide should invest in Internet safety by supporting programs aimed at increasing public awareness of Internet risks and guidance to help people avoid those risks.

ENCOURAGE INNOVATION AND SELF-REGULATION As governments address the risks associated with emerging technologies and online services, it is important that they support industry self-regulation and legislative frameworks that foster an environment of technological innovation, as well as promote cooperation between government and the technology industry.

Combating Child Exploitation Online

Key Points

- The Internet serves many beneficial and constructive purposes, but it has also created avenues for criminals to exploit young people through the distribution of child sex abuse images and the trafficking of children for sexual purposes.
- Microsoft aids in the advancement of technology, techniques, and processes to combat the use of the Internet to exploit children. These efforts include the development of technology (like Microsoft PhotoDNA) that can detect images of child exploitation, as well as partnerships with law enforcement agencies and nongovernmental organizations devoted to the cause.
- It is essential to enact and enforce laws against the possession, production, and distribution of child pornography worldwide, and to both build and fund the necessary infrastructure to ensure safe rescue, support, and recovery for victims of child sexual exploitation.

Every day, millions of people connect and share content on the Internet in beneficial and constructive ways. But the Internet has also created new avenues for criminals to exploit young people, such as through the distribution of child sex abuse images (also known as child abuse images), the trafficking of children for sexual purposes, and the grooming of children for sexual exploitation.

The production and distribution of child pornography represents a significant global law enforcement problem. Since 2002 (when its Child Victim Identification Program was created), the National Center for Missing & Exploited Children (NCMEC) has reviewed and analyzed more than 96 million images and videos of child sex abuse. These images are often found after pedophiles share and trade them amongst themselves and with others who reinforce their shared sexual interest in children.

As of 2011, most of the child pornography victims identified by NCMEC were prepubescent, with infants and toddlers the fastest-growing age category. Internet companies have an important role to play in helping fight this horrific trade by acting quickly to find, report, and eliminate these illegal images.

Another form of child exploitation is child predators' use of the Internet to find victims. These predators take advantage of the Internet's anonymity to build online relationships with young people or to communicate with those who traffic children for sex. As in the fight against images of child sex abuse, Internet companies have an important function in stopping predators and child sex traffickers. They can enforce codes of conduct, provide mechanisms for customers to report predators, and invest in innovation for improved detection.

Globally, law enforcement is doing admirable work to combat the online exploitation of children, but the scale of this problem requires broader cooperation from law enforcement, government, industry, nongovernmental organizations, and academia.

Microsoft Approach

COMBATING CYBERCRIME The Microsoft Digital Crimes Unit is an international legal and technical team working with partners to address technology-facilitated crime. With the opening of the Cybercrime Center in late 2013, Microsoft brought its cybercrime experts— attorneys, investigators, business professionals, and forensic analysts from around the world—together under one umbrella to help them better coordinate and collaborate to address cyberthreats.

COMBATING ILLEGAL IMAGES

- Microsoft applies filtering tools and employs highly trained experts using cutting-edge technology to help detect and classify images of child abuse that are shared on Microsoft services, such as Bing. The company reports these images to NCMEC, removes them, and bans the perpetrators from the services.

- In 2009, Microsoft Research collaborated with Dartmouth College and NCMEC to develop an advanced technology called PhotoDNA, which helps to refine and automate the search for child sex abuse images among the billions of photos on the Internet. NCMEC used the PhotoDNA license to work with online services such as Facebook to uncover images of child abuse. Since then, it has become the industry standard for detecting such images.

PARTNERING WITH OTHERS Microsoft partners with law enforcement and others around the world.

- In 2012, Microsoft worked with NetClean to make PhotoDNA image-matching technology available to law enforcement at no cost, in order to aid in investigations of the sexual exploitation of children.

- The company collaborates with the Thorn Technology Task Force (whose members also include Facebook, Twitter, and Google) to explore new ways technology can address the problem of child exploitation.

- In 2011, Microsoft issued a request for proposals for academic research into the role of technology in the sex trafficking of children. In 2012, Microsoft distributed $185,000 to six winning teams whose research results will be released as they are completed in 2014.

Policy Considerations

Policymakers can help address the challenges of combating child exploitation online by supporting the following efforts:

SUPPORT VICTIM RECOVERY SERVICES. Funding and infrastructure for effective victim recovery services is absolutely essential. Without this, any other interventions have the potential to do more harm than good.

ENACT LAWS THAT PROTECT VICTIMS OF CHILD EXPLOITATION It is vital that governments enact and enforce:

- Child exploitation laws that recognize and protect victims while holding traffickers accountable.

- Laws against the possession, production, and distribution of child sex abuse images worldwide. In 2012, the International Centre for Missing & Exploited Children (ICMEC) reported that 100 countries have "enacted new laws to protect children from child pornography." However, 53 countries have no laws at all, and 127 countries do not have laws that ICMEC considers sufficient.[11]

SUPPORT INDUSTRY-WIDE BEST PRACTICES AND GUIDANCE Internet companies must continue to work with governments and law enforcement to help address the problem of online predators by establishing industry best practices and guidance. More emphasis must be placed on enabling companies to voluntarily find and report images of child sex abuse. Policymakers can help change the focus of law enforcement to a model that measures their activities to stop crime and prevent abuse without penalizing the victim.

11 *ICMEC 2012 Highlights:* www.icmec.org/en_X1/icmec_publications/ICMEC_Highlights_2012.pdf

Combating Child Grooming Online

Key Points

- Grooming, the process by which predators manipulate children for sexual exploitation, is facilitated online when sexual predators use the Internet to make contact and develop relationships with children.
- The Microsoft approach to combating child predation includes creating innovative technology tools; providing education and guidance; establishing robust internal policies and practices for moderating content and addressing online abuses; and partnering with government, industry, law enforcement, and others.
- Microsoft strongly supports enacting and enforcing laws against the sexual exploitation of children, and cooperates with law enforcement to bring Internet pedophiles to justice.

Child grooming is a process of emotional manipulation by which pedophiles prepare children and youth for sexual exploitation. The grooming process typically involves an adult befriending a young person and then winning his or her trust by showering the youth with flattery, sympathy, gifts of money or modeling jobs, and other personal attention. The groomer then tries to sexualize the relationship, seeking to control the child and continue the abuse, which may include images of child sexual abuse or sex trafficking.

Pedophiles go where children go, and today that includes the Internet. Child grooming goes online when pedophiles use the Internet for the grooming process. Adults may begin the grooming process by visiting forums where youth interact, such as online games (which may use two-way voice and video technology) or chat rooms, or they may contact children through text messages. Pedophiles use the information that children reveal about themselves online to target vulnerable youngsters with low self-esteem, family or social issues, or lack of resources.

Sexual exploitation of children is a global problem. However, it is important to keep the online portion of the problem in perspective. According to the Crimes Against Children Research Center in the United States, the arrest of more than 600 online predators in 2006 constituted about one percent of all arrests for sex crimes committed against children and youth.

Internet companies have an important role to play in helping to stop predators. They can enforce codes of conduct, deploy monitors in forums used by children, and provide mechanisms for customers to report inappropriate conduct.

Microsoft Approach

The Microsoft approach to combating child grooming online includes developing technology, providing guidance, establishing internal policies, and partnering with others.

CREATING TECHNOLOGY TOOLS Microsoft builds safety features into a wide range of its products and services to help parents watch over their children online. For example, Windows 8 Family Safety offers tools to help parents monitor their children's online activities. Anyone—adult or young person—with a Microsoft account can specify who can view their profiles or contact them. In addition, Xbox Live has Online Safety Settings that enable parents to restrict who children can communicate with and who can see their profiles or friends lists.

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center provides age-based guidance for Internet use, including tips on teaching children what's appropriate to view and share online; how to stay safer on mobile devices and in online games; and how to avoid, block, and report inappropriate behavior.

ESTABLISHING INTERNAL POLICIES AND PRACTICES To protect users on its online services, Microsoft enforces policies inherent in its code of conduct for users of its online services (such as Xbox Live), and moderates content and interactions to address illegal activity, inappropriate material, and other abusive content or contact.

PARTNERING WITH OTHERS Combating child predation requires a holistic approach in which technology providers, government leaders, law enforcement, and nongovernmental organizations all play vital roles.

- The Microsoft Digital Crimes Unit is an international legal and technical team working with partners to address technology-facilitated crime. With the opening of the Cybercrime Center in late 2013, Microsoft brought its cybercrime experts—attorneys, investigators, business professionals, and forensic analysts from around the world—together under one umbrella to help them better coordinate and collaborate to address cyberthreats.

- In 2009, Microsoft Research collaborated with Dartmouth College and the National Center for Missing & Exploited Children (NCMEC) to develop PhotoDNA, an advanced image-matching technology that helps to refine and automate the search for child sex abuse images among the billions of photos on the Internet. NCMEC used the PhotoDNA license to work with online services, such as Facebook, to uncover images of child abuse. Since then, it has become the industry standard for detecting online images of child abuse.

- Microsoft works with NCMEC, INTERPOL, and other organizations to encourage governments to combat child predators.

Policy Considerations

Policymakers can help address the challenges of combating child grooming online by supporting the following efforts:

STRENGTHEN AND ENFORCE EXISTING CHILD PROTECTION LAWS Governments must enact and enforce laws against the sexual exploitation of children, including the possession, production, and distribution of child sex abuse images.

SUPPORT INDUSTRY-WIDE BEST PRACTICES Internet companies should work with governments and law enforcement to help combat online child predation by giving their customers mechanisms for reporting potential predators, enforcing codes of conduct, and spurring further innovation to help reduce illegal or inappropriate content and conduct.

SUPPORT INTERNET SAFETY RESEARCH It is essential that governments commission studies and fund academic and industry research to advance Internet safety. Research is particularly important for identifying factors that increase online risks and for dispelling myths that can lead to misplaced efforts to advance Internet safety.

Combating Human Trafficking Online

Key Points

- Although technology can be used to facilitate the horrific practice of human trafficking, technology can also be used to help combat it.
- Microsoft applies its experience in addressing technology-based crime and invests in research, partnerships, policies, and best practices to support human rights and advance the fight against human trafficking.
- Issues related to human trafficking are complex and require a multi-part solution, including strong public-private partnerships, effective infrastructure for victim support, and intervention efforts founded in solid research.

Human trafficking includes commercial sexual exploitation, forced labor, and other forms of modern-day slavery. Technology can play a role in facilitating—and also combating—these horrific human rights abuses. Although academics are increasingly exploring this area, today there remains insufficient research data to determine the extent to which technology is increasing human trafficking, or the way in which law enforcement and nongovernmental organizations can use technology to better disrupt it.

However, for any intervention efforts to be successful rather than unintentionally cause further harm, it is essential that victims receive the services and support they need when they are recovered from trafficking situations. Assuming that broader systemic progress can be made in ensuring this necessary support for victims, advances in research may lead to future opportunities for effectively using technology to help address trafficking.

Anti-trafficking advocates, law enforcement agencies, and governments around the world have long worked to combat human trafficking. Microsoft believes that technology companies also have an important role to play in driving deeper research and innovation to use technology to more effectively disrupt the business of trafficking people.

Microsoft Approach

Microsoft recognizes its responsibility as a global corporate citizen to respect human rights and aid in the fight against human trafficking. The company expresses its commitment in the human rights statement it released in July 2012 in accordance with the United Nations Guiding Principles on Business and Human Rights.

Microsoft established the Technology and Human Rights Center to help ensure that it meets its commitment to respect human rights. The Center works to advance public understanding of the impact of information and communications technology on human rights. It also aims to coordinate strategic engagement in public policy debates relating to law enforcement, technology, and surveillance to encourage policies that protect human rights.

Microsoft also reflects its commitment to combating human trafficking by investing in research and innovation; establishing partnerships with anti-trafficking advocates and law enforcement agencies worldwide; and implementing policies and best practices to help prevent its technologies from contributing to exploitation.

INVESTING IN RESEARCH AND INNOVATION Microsoft invests in research to develop a more accurate understanding of the role that technology plays in human trafficking, particularly child sex trafficking.

In 2011, Microsoft issued a request for proposals for academic research into the role of technology in the sex trafficking of children. In 2012, the company distributed $185,000 to six winning teams whose research results will be released as they are completed in 2014.

Microsoft Research is collaborating with the Harvard Kennedy School of Government and the University of Southern California Annenberg School on additional related research.

Microsoft works with leading technology institutions and nongovernmental organizations on efforts such as the International Women's Hackathon, which helps foster technology innovation designed to address trafficking.

ESTABLISHING PARTNERSHIPS Microsoft works with anti-trafficking advocates and law enforcement agencies worldwide to help address human trafficking. Through cooperative efforts that raise the cost, risk, and difficulty of doing business for human traffickers, Microsoft can help make it a less lucrative, and therefore less appealing, trade.

Law enforcement, nongovernmental organizations, and other technology companies like Facebook and NetClean use PhotoDNA, an image-matching technology developed by Microsoft and Dartmouth College to help identify images of child abuse.

Microsoft collaborates with the Global Business Coalition Against Trafficking, the White House Office of Science and Technology Policy, the Council on Women and Girls, United Nations Global Initiative to Fight Human Trafficking (UN.GIFT), US state attorneys general, and local police agencies.

As a founding member of the Thorn Technology Task Force, Microsoft collaborates with Facebook, Twitter, Google, and others to explore new ways technology can address the problem of child sex trafficking.

Microsoft supports organizations such as the Polaris Project, International Centre for Missing and Exploited Children (ICMEC), and the International Justice Mission, all of which combat trafficking and support trafficking victims.

IMPLEMENTING POLICIES AND BEST PRACTICES Microsoft works to help prevent its technologies and processes from contributing to exploitation in its operations and those of its suppliers.

All companies doing business with Microsoft must agree to abide by the company's Vendor Code of Conduct, which outlines required ethical business practices, including an explicit prohibition of the use of forced labor.

For its hardware manufacturers and packaging suppliers, Microsoft has invested in a social and environmental accountability program, which includes independent third-party audits to help ensure compliance with its Code of Conduct and local and national regulations. If these standards are not met, suppliers risk remedial action, including termination of their contracts.

Policy Considerations

Governments and policymakers can help address the problem of human trafficking by focusing on the following priorities:

- **CREATE AND ENFORCE STRONG ANTI-TRAFFICKING LEGISLATION** It is vital that governments enact and enforce human trafficking laws that recognize and protect victims while holding traffickers accountable.

- **PROVIDE FUNDING AND INFRASTRUCTURE** Funding and infrastructure for effective victim recovery services is absolutely essential. Without this, any other interventions have the potential to do more harm than good.

- **ENCOURAGE COLLABORATION ON INITIATIVES** Researchers and technology companies should continue to work with governments, law enforcement, and those in the anti-trafficking community to help understand and address the abuses of technology that facilitate trafficking, adopt effective intervention techniques based on research, and develop anti-trafficking initiatives.

Combating Online Bullying

Key Points

- Online bullying has long been a problem; taking it online has opened the door to 24-hour hurt.
- Microsoft promotes efforts to combat online bullying by creating technology tools, enforcing policies against abuse in its online services, providing education and guidance, and establishing partnerships with others.
- Governments play a vital role in helping to combat harassment and threats online through laws that are thoughtfully written, balancing safety and freedom of speech.

Bullying among youth has long been a serious problem. Just like bullying in person, online bullying (also known as *cyberbullying*) is repeated behavior intended to tease, demean, or harass someone less powerful. Young people can bully using any type of Internet-connected device through text and instant messaging, games, or social media such as Facebook and Tumblr. Bullying online opens the door to 24-hour hurt, which can be amplified by anonymity and the potential for broadcast to a wide audience.

There are many reasons why young people mistreat others, whether out of boredom, to get approval or be funny, to retaliate for having been bullied themselves, or because they are in distress. It isn't always intentional—what starts as an argument may escalate. Often, young people may not even recognize their behavior as bullying, rather referring to it as *drama*.[12]

Because young people practically grow up online, it's no surprise that bullying has moved to the Internet. Estimates of the prevalence of online bullying vary. However, in 2012, a Microsoft study of more than 7,500 children ages 8-17 in 25 countries found that 37 percent of those interviewed had experienced meanness online and 24 percent had bullied someone online.[13]

Youth who experience online bullying—whether as one who bullies, who is the target of bullying, or who is a bystander—can suffer damaging mental health consequences. According to the Cyberbullying Research Center, "research reveals a link between online bullying and low self-esteem, family and academic problems, school violence, and delinquent behavior."

Two challenges make stopping online bullying difficult. First, many do not regard it as a serious form of aggression. And second, cyberbullying incidents can slip through the cracks. The Cyberbullying Research Center reports that, "Parents often say that they don't have the technical skills to keep up with their kids' online behavior; teachers are afraid to intervene in behaviors that often occur away from school; and law enforcement is hesitant to get involved unless there is clear evidence of a crime or a significant threat to someone's physical safety."[14]

To address online bullying, everyone—youth, parents, educators and counselors, law enforcement, technology companies, and the community at large—must together create an environment where young people feel comfortable talking with adults about this problem, safe enough as bystanders to get involved, and confident that meaningful steps will be taken to resolve it.

---

12 The Drama! Teen Conflict, Gossip, and Bullying in Networked Publics: **aka.ms/teen_drama**
13 Online Bullying Among Youth 8-17 Worldwide: **aka.ms/OBResearch**
14 Cyberbullying Identification, Prevention, and Response, Cyberbullying Research Center: **www.cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf**

Microsoft Approach

CREATING TECHNOLOGY TOOLS Microsoft provides technology tools that can be tailored to each child. Parent can monitor their children's web activity and block unwanted contact using Family Safety on Windows 7 and Windows 8 or monitor kids' phone use in Kid's Corner on Windows Phone. For young gamers, parents can use Online Safety Settings for Xbox Live to specify what activities children can participate in, who they can communicate with, and who can see their profile.

ESTABLISHING INTERNAL POLICIES AND PRACTICES Microsoft enforces policies against abuse and harassment on its online services—for example, through the Code of Conduct on Xbox Live—and moderates content and interactions to address any abuse, illegal activity, or inappropriate material. Customers who misuse Microsoft services are subject to account termination; serious incidents may be reported to law enforcement.

PROVIDING EDUCATION AND GUIDANCE Microsoft produces educational materials for teachers and parents to teach young people how to stand up to online bullying, what to do if a child is involved in it, and how to promote a culture of kindness, which research shows to be a potent way to help stop bullying.

PARTNERING WITH OTHERS Microsoft works with governments, industry groups, and others to help address online bullying through efforts like GetNetWise in the United States and Insafe in the European Union.

Policy Considerations

BALANCE ANTI-HARASSMENT LEGISLATION WITH FREE SPEECH RIGHTS Governments play a vital role in helping to combat online harassment and threats through laws that are thoughtfully written to balance safety and freedom of speech.

PROMOTE COMPREHENSIVE ONLINE SAFETY EDUCATION IN SCHOOLS Government support for anti-bullying education, as part of a comprehensive online safety curriculum for elementary and secondary school students, can provide a foundation for addressing the problem of online bullying. One example of such support is a US law mandating that anti-bullying measures be taught in any school that receives E-Rate funding from the Federal Communications Commission (FCC). (The E-Rate program gives schools and libraries discounts for telecommunications and Internet access.[15])

ENCOURAGE INDUSTRY COOPERATION Microsoft supports legislation that releases access providers from liability for obscene material or abusive behavior if they have made a good-faith effort to screen their services or provided screening devices for parents. Examples include Section 230 of the US Communications Decency Act and the European Union Directive 2000/31/EC.

15 *Laws Require Internet Safety Education in Schools that Receive E-Rate Funds:* www.safeschools.info/bullying-prevention/bullying-prevention-news/362-laws-require-internet-safety-education-in-schools-that-receive-e-rate-funds

Combating Online Fraud

Key Points

- Online fraud is a significant global problem, victimizing millions of unsuspecting consumers each year. In the United States alone, the FBI's Internet Crime Complaint Center recorded just under 300,000 fraud complaints in 2012 with an adjusted dollar loss of US$525 billion.
- Microsoft takes a four-part approach to combating online fraud: dedicating internal teams to fighting cybercrime; developing technology tools; producing education and guidance; and promoting relationships with government, industry, law enforcement, and others.
- Microsoft supports government efforts to fight online fraud through international cooperation, public-private partnerships, and strong enforcement of anti-fraud laws.

The Internet has transformed commerce around the world, building new companies and services and enabling consumers to engage in a wide variety of economic activities. Total global e-commerce sales were projected to exceed US$1.2 trillion in 2013.

However, as economic activity moves increasingly online, so has the problem of fraud, which threatens to undermine the public trust in the benefits of e-commerce. Online fraud is a significant global problem. In the United States alone, the FBI's Internet Crime Complaint Center recorded just under 300,000 fraud complaints in 2012, with an adjusted loss of US$525 billion.

Organized cybercriminals go to great lengths to execute their online schemes in order to steal identities or carry out financial fraud. Criminals lure their victims using such devious tactics as social engineering, phishing, malicious software (or *malware*), and more.

Social engineering takes advantage of people's trust by tricking them into actions such as installing malware disguised as a legitimate app or entering sensitive personal information on a convincing but fake website—actions that can compromise their devices and data.

Phishing scams use email, text, social network messages, or even phone messages that appear to come from a reputable organization; they aim to entice victims to disclose sensitive information, such as account numbers or passwords. In its most recent account, the Anti-Phishing Working Group reported almost 280,000 unique phishing attacks worldwide between June 2012 and June 2013, with the number of brands exploited by phishers at an all-time high.

To combat online fraud successfully, businesses, government, nongovernmental organizations, and consumers worldwide must work together.

Microsoft Approach

DEDICATED INTERNAL TEAMS The Microsoft Digital Crimes Unit is an international legal and technical team working with partners on such issues as malware and intellectual property (IP) crimes as well as technology-facilitated child exploitation. The team applies its legal and technical expertise to help enhance cloud security and create a safer digital world.

With the opening of the Cybercrime Center in late 2013, Microsoft brought its cybercrime experts from the areas of IP crime, botnets, malware, and child exploitation together under one umbrella. When crimes cross these focus areas—as is happening with greater frequency (for example, the Nitol and Citadel botnets)—Microsoft experts can better coordinate and work together to address cyberthreats. The combined team includes more than 100 attorneys, investigators, business professionals, and forensic analysts based around the world.

TECHNOLOGY TOOLS Microsoft offers many tools to help consumers fight online fraud:

- Microsoft Security Essentials is a free program that provides real-time protection against viruses, spyware, and other malware.
- The SmartScreen Filter is a feature in Internet Explorer that helps warn consumers about potential phishing websites and helps protect against the installation of malware. SmartScreen antispam filters are built into Microsoft email programs to help protect customers from messages that may contain fraudulent solicitations.
- The Microsoft Malicious Software Removal Tool checks computers running the most recent versions of Windows for specific malware and then helps remove any infections it finds.
- The Microsoft Safety Scanner is a free tool that provides on-demand scanning and helps remove malware.

EDUCATION AND GUIDANCE The Microsoft Safety & Security Center offers advice to help consumers protect themselves against online fraud, including tips on how to recognize phishing scams and protect against identity theft.

PARTNERSHIPS Microsoft works with many organizations dedicated to fighting online fraud, including the Anti-Phishing Working Group and the National Cyber Security Alliance.

Policy Considerations

Governments can aid in fighting Internet fraud and other cybercrime by supporting the following efforts:

SUPPORT ADOPTION OF 2001 COUNCIL OF EUROPE CONVENTION ON CYBERCRIME Microsoft has joined with industry to encourage countries to adopt and ratify the 2001 Council of Europe Convention on Cybercrime,[16] which requires signatories to adopt and update laws and procedures to address online crime.

BALANCE REGULATION WITH INNOVATION Although it is essential to enact laws against online fraud and enforce the prosecution of cybercriminals, anti-fraud legislation must be carefully crafted so as not to discourage innovation and technology adoption in the process.

ENCOURAGE PUBLIC-PRIVATE PARTNERSHIPS Public and private relationships are essential to addressing the increasing complexities of cybercrime. For example, Microsoft gives technical training to law enforcement agencies worldwide, develops new technologies to combat cybercrime, and has helped protect consumers by taking legal action.

16 *Convention on Cybercrime, 2001:* conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Safer Online Gaming

Key Points

- Online gaming offers a wide variety of content for many audiences, but not all games and apps are appropriate for everyone. Concerns about harmful effects can be addressed through parental involvement and family education, along with such industry rating systems as ESRB, PEGI, and CERO.
- The Microsoft approach to safer, more trusted gaming experiences includes creating technology tools; providing education and guidance; developing internal policies and practices for moderating content and addressing online abuse; and partnering with government, industry, law enforcement, and others.
- The combination of voluntary industry rating systems, family education, and parental involvement offers the best solutions for making informed decisions about game content.

Gaming, whether on a gaming console, tablet, or mobile phone, offers a wide variety of content for many audiences. However, not all games and apps are appropriate for (or acceptable to) everyone, and many people have expressed concern about their potential harmful effects on children. Some governments have responded to these concerns by restricting access to or even banning certain video games because of sexually explicit or violent content.

The gaming industry has taken the initiative by adopting voluntary rating systems. These include the Entertainment Software Ratings Board (ESRB) ratings in the United States, the Pan European Game Information (PEGI) ratings in more than 28 European countries and Israel, and the Computer Entertainment Rating Organization (CERO) in Japan. The industry recognizes that additional tools are needed to help inform consumers. In response, an international working group that includes Microsoft is developing the International Alliance for Rating Content (IARC), a global ratings framework that will enable game developers to apply in one place for game ratings for many rating systems.

These widely recognized rating systems provide descriptive information about game content, which merchants are encouraged to display and which parents can use as a guide to help inform their content decisions. A 2012 report found that one of every two European consumers recognize PEGI labels,[17] and a 2013 ESRB survey found that 75 percent of US parents "regularly check a game's rating before making a purchase."[18] A "secret shopper" program by the US Federal Trade Commission (FTC) in 2013 found that 87 percent of US merchants refused to sell games with a mature rating to a minor.[19]

No matter what games and apps a family decides are suitable, it is vital that parents take an active interest in and understand the ever-changing digital world that captivates children's attention and imagination. Parents should decide what content—be it game, app, music, movie, or television show—is appropriate for their family, and then take the steps they need to set limits based on those choices. To do this, parents must understand the rating systems and technology tools like family safety settings that can help them set those limits.

---

17 Pan European Game Information (PEGI) Annual Report 2012: **www.pegi.info/en/index/id/1068/nid/media/pdf/390.pdf**

18 ESRB Survey: Parental Awareness, Use & Satisfaction: **www.esrb.org/about/awareness.jsp**

19 FTC Undercover Shopper Survey, March 25, 2013: **www.ftc.gov/news-events/press-releases/2013/03/ftc-undercover-shopper-survey-entertainment-ratings-enforcement**

Microsoft Approach

The Microsoft approach to encouraging more trusted gaming experiences includes creating technology tools, providing guidance, developing internal policies and practices for moderating content and addressing online abuse, and collaboration.

CREATING TECHNOLOGY TOOLS

- Xbox 360 Family Settings enable parents to set and enforce content ratings for games, movies, and television shows; set a pass code to restrict who can change these settings; and set limits on console play time using the family timer.

- On Xbox One, parents use Family and Online Safety controls to specify a maximum age that maps to game ratings. Parents can then decide whether they want Xbox One to always block content that exceeds this rating or make that decision on a case-by-case basis.

- Online Safety Settings for Xbox Live enable parents to create individual profiles that are appropriate for each child's age and maturity. Parents can specify what activities children can participate in (such as multiplayer gaming, video chat, text messaging, or voice messaging), who they can communicate with, and who can see the child's profile or friends list. In addition, Xbox Live supports a reputation system that encourages healthy participation in games while diminishing the reputation of troublemakers and cheaters.

- Windows Phone 8 offers two ways to manage the access of young people to games and apps.

    - Young people under age 18 who have their own Windows Phone sign in with a child's account. They won't be able to download anything until parents set up My Family and add the young person. Once that's done, parents can manage the apps and games that the young person can download from the Windows Phone Store and use the game-rating filter to limit access.

    - For younger ones, parents can use Kid's Corner to create a space on their phone where children can play games, use apps, listen to music, and watch videos that parents have selected.

PROVIDING EDUCATION AND GUIDANCE The work of Microsoft is incomplete if consumers do not know how to use the technology and other resources that are available to help protect young gamers. Microsoft provides educational materials in the Microsoft Safety & Security Center and in the Xbox Live Healthy Gaming Guide.

DEVELOPING INTERNAL POLICIES AND PRACTICES Microsoft develops company-wide policies, standards, and procedures for its products and services that connect with the Internet. The company enforces a code of conduct for users of its gaming services like Xbox Live, and moderates content and interactions to help address any abuse, illegal activity, or inappropriate material.

PARTNERING WITH NONGOVERNMENTAL ORGANIZATIONS, INDUSTRY, AND GOVERNMENT Creating a safer gaming environment requires a holistic approach in which safety advocacy groups, government leaders, and technology providers all play vital roles. Central to Microsoft efforts is engaging—through public policy—with governments around the world and with organizations such as the National Cyber Security Alliance and the Family Online Safety Institute.

Policy Considerations

Government and industry policymakers can help improve safety in online gaming by supporting the following efforts:

- **ENCOURAGE RATING SYSTEMS AND PARENTAL INVOLVEMENT INSTEAD OF MANDATORY COMPLIANCE** The combination of voluntary industry rating systems, family guidance, and parental involvement provides the best solutions for addressing concerns about gaming and other online entertainment. Microsoft also supplies funding and technical expertise in the development of IARC, a best practice that is supported by nongovernmental organizations and rating agencies, both national and independent.

- **PROMOTE INNOVATION AND CONSUMER EDUCATION** In a vibrant ecosystem, game and app developers and publishers should be able to create products and content for customers of all ages. At the same time, these technology businesses must give parents and caregivers the information and tools they need to make informed decisions about the quality and appropriateness of the interactive games and apps that their children play and use.

Online Reputation

Key Points

- Managing an online reputation is important—it can have a significant impact on a person's life in a number of ways, including employment prospects, relationships, and college admissions.
- Microsoft helps its customers cultivate and protect their online reputations by offering relevant education and guidance, establishing internal policies that help customers better manage their content, and creating technology tools.
- Governments must balance the obligation to help citizens protect their online reputations with the right of free expression.

Worldwide, people are living more of their lives online than ever before. It's where many go to promote themselves, spend time with friends, and find employment, education—even a spouse. A 2012 survey of 19,000 respondents in the United States who had married between 2005 and 2012 found that a third had met online.[20] Research in 2013 by the Dutch dating site, Meetic, found that one in five in the Netherlands was in a long-term relationship that had originated online.[21] Since 2010, nearly three-quarters of US job seekers have used the Internet to find employment.

Research also shows that the information that appears about an individual online can have a significant impact on that person's prospects for employment and education. Microsoft research[22] in 2009 found that 70 percent of US hiring managers and 41 percent of UK hiring managers had rejected a candidate because of information found online. A 2012 survey[23] found that 35 percent of admissions officers in the United States "discovered something that negatively impacted an applicant's chances of getting into the school."

Because a simple online search can reveal a great deal about a person, there is increasing interest in online reputation, and in particular, one's digital footprint—the trail left by online activities such as blogging, posting comments or pictures, gaming, and social networking. While a positive digital footprint can enhance a person's employment opportunities and other prospects, a negative one caused by inappropriate photographs or rude comments left online can damage those possibilities. Users of social networking services may reveal details about their lives that are more lasting and available to a wider audience than they may realize, with consequences for their reputations that they may not imagine. It is essential then for consumers to understand the risks and take appropriate steps to protect their reputations.

In 2011, a Microsoft survey[24] of 5,000 adults and children in Canada, Germany, Ireland, Spain, and the United States found that 90 percent have done something to manage their online profile, but only 44 percent actively think about the long-term consequences that their activities have on their online reputation.

20 Marital satisfaction and break-ups differ across on-line and off-line meeting venues. John Caioppo, et. al., University of Chicago, December 2012: **www.pnas.org/content/early/2013/05/31/1222447110**

21 Research on the dating market in The Netherlands: **www.datinginsider.nl/research-on-dating-market-in-the-netherlands-more-than-20-had-a-relationship-that-started-online**

22 Online Reputation in a Connected World, 2009: **www.microsoft.com/security/resources/research.aspx#reputation**

23 Kaplan Test Prep's 2012 Survey of College Admissions Officers: **press.kaptest.com/research-and-surveys/kaplan-test-preps-2012-survey-of-college-admissions-officers**

24 Online Reputation Management: Parents and Children 8-17, 2011: **www.microsoft.com/security/resources/research.aspx#onlinerep**

Microsoft Approach

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center offers advice to consumers on how they can cultivate and protect their online reputations, safeguard their privacy, and avoid, block, and report inappropriate behavior.

ESTABLISHING CONTENT MANAGEMENT POLICIES Microsoft has established content management policies on its sites:

- The Microsoft Terms of Use do not allow customers to "publish, post, upload, distribute or disseminate any inappropriate, profane, defamatory, obscene, indecent or unlawful ... materials," or to "defame, abuse, harass, stalk, threaten or otherwise violate the legal rights ... of others."
- The Microsoft Services Agreement states that "Microsoft may remove your content without asking you if we determine it's in violation of this agreement or the law."

CREATING TECHNOLOGY TOOLS Microsoft offers features that help customers manage their digital footprint in its products and services.

- The Microsoft Personal Data Dashboard—a central location for personal information associated with selected Microsoft products —helps customers control how that information is displayed.
- Internet Explorer offers settings to help people manage their privacy online, including InPrivate browsing. People who use this feature browse as usual, but when they close Internet Explorer, InPrivate deletes passwords, search history, webpage history, and other data.
- The Smart Match feature in Xbox Live matches players in part based on their reputation, reducing the impact that misconduct has on the Xbox Live community.

Policy Considerations

BALANCE REGULATION WITH FREEDOM OF EXPRESSION In crafting legislation, governments must balance the obligation to help citizens protect their online reputations with the right of free expression.

SUPPORT INDUSTRY-LED EDUCATION AND GUIDANCE Technology companies can help their customers cultivate and protect their online reputations by offering relevant education and guidance and by creating policies that help people better manage their content and privacy.

ENCOURAGE INTERNET INDUSTRY COOPERATION Policymakers should support legislation that releases access providers from liability for obscene material or abusive behavior if they have made a good-faith effort to screen their services or provided screening devices for parents. Examples include Section 230 of the US Communications Decency Act and the European Union Directive 2000/31/EC.

Online Safety for Mobile Devices

Key Points

- As the wireless economy expands, so do incentives for (and risks created by) cybercriminals who use malware to steal identities, money, and business data.
- To reduce the risk on mobile devices and help create safer, more trusted mobile computing experiences, Microsoft develops technology tools; provides education and guidance; and partners with government, industry, law enforcement, and nonprofit organizations.
- As governments address the risks of emerging technologies, they must avoid top-down regulation that stymies technology adoption and preserve flexibility so that industry can innovate. In addition, government and industry must collaborate to support and promote mobile safety education for people of all ages.

Mobility is the cornerstone of the twenty-first century connected world, and mobile devices are ubiquitous, fueled by their power, convenience, and always-on connectivity. For example, 91 percent of all the people on earth have a mobile phone (up from 83 percent in just two years)—more than half (56 percent) of those have a smartphone.[25] In fact, in its Visual Networking Index,[26] Cisco predicts that by 2014 there will be more mobile-connected devices in the world than there are people.

Usage of mobile devices is also expanding. Today, 60 percent of mobile web users worldwide use their mobile device as the primary or exclusive means of going online, and Cisco anticipates that mobile data traffic will grow more than 11-fold between 2013 and 2018.

However, as the wireless economy expands, so do incentives for (and threats from) cybercriminals, whose ultimate goal is to profit from spying on users. According to the *Kaspersky Security Bulletin 2013*,[27] mobile malicious software is one of the fastest-developing IT security risks, doubling in the first six months of 2013.

People's mobile devices hold tremendous amounts of personal (and often business) data, and criminal activity puts these at risk through malware that is designed especially to steal sensitive data from mobile devices, theft of the device itself, or use of unsecured wireless networks to send sensitive information. Mobile botnets are especially destructive because mobile devices are almost always on, so they're reliably available for new instructions from the botnet controller.

Mobile users may suffer identity theft and financial loss. Businesses also stand to lose customer data and intellectual property if personal mobile devices (including flash drives) are used at work and not adequately protected. In addition, personal privacy can be compromised if the location-based data on a mobile device—collected through its GPS or nearby Wi-Fi access points and cell towers—is shared publicly.

Industry invests in innovative solutions to protect device firmware and software from attack. Consumers can also protect themselves and their devices by taking simple steps, so the need is greater than ever for safety training.

Microsoft Approach

DEVELOPING TECHNOLOGY TOOLS Microsoft builds in technology to help protect the data and privacy of mobile users:

25 Infographic: 2013 Mobile Growth Statistics: **www.digitalbuzzblog.com/infographic-2013-mobile-growth-statistics/**

26 Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018: **www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html**

27 Kaspersky Security Bulletin 2013: **www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013**

- Windows Defender helps guard tablets and laptops against all kinds of malware in real time, and Windows SmartScreen helps warn consumers about potential phishing websites. Parents can use the Family Safety feature in Windows to create a separate account for each family member, enabling them to monitor children online and set specific activity limits.

- Internet Explorer offers settings, including InPrivate browsing, that help users manage their privacy online. People using this feature browse as usual, but when they close Internet Explorer, InPrivate deletes passwords, search history, webpage history, and other data.

- Through the Windows Phone Store, Microsoft works with mobile service providers and independent software companies to give consumers reputable mobile safety apps that can block web-based threats, provide contact management for children, and more. Windows Phone also offers Kid's Corner, where parents can set limits on access to apps, games, and music.

- Windows Phone apps that use location data are required to give customers the ability to turn off that app's access to an individual's location. The Windows Phone location service does not store any unique device identifiers or data that personally identifies users or that would allow tracking or creation of the location history of a device.

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center offers advice on how to use devices more safely, which includes locking phones with PINs or strong passwords, guidance for safe use of public Wi-Fi hotspots and location-based features, and specific advice for kids.

ESTABLISHING PARTNERSHIPS Building greater safety and security requires a holistic approach in which government leaders, law enforcement, technology providers, and nongovernmental organizations collaborate. Microsoft works with industry and others through such organizations as the GSM Association and CTIA–The Wireless Association.

Policy Considerations

SUPPORT FLEXIBLE, BALANCED LEGISLATION THAT ALLOWS FOR INNOVATION As governments address risks associated with emerging technologies and online services, they must also avoid top-down regulation that stymies technology adoption, and preserve flexibility so that industry can innovate. In addition, government and industry must collaborate to establish mobile safety principles to help build a more secure Internet.

ENCOURAGE INDUSTRY BEST PRACTICES AND GUIDELINES Mobile providers should establish voluntary guidelines and best practices that address such issues as content classification, location-based services, and mobile commerce in order to help people make informed decisions about their safety.

SUPPORT COMPREHENSIVE MOBILE SAFETY EDUCATION Governments must work with information and communications providers, online safety organizations, and school districts to provide mobile safety education for consumer and business users, and to promote safety curricula that addresses mobile safety for young people.

Safer Social Networking

Key Points

- Social networks are highly popular and offer enriching experiences, but they may involve such risks as exposure to malicious software, potential loss of privacy, harassment, online bullying, and damage to one's reputation.
- The Microsoft approach to helping people manage their safety and privacy on social networks includes creating technology tools; providing education and guidance; developing internal policies and practices for moderating content and addressing online abuses; and partnering with government, the technology industry, nongovernmental organizations, and others.
- Governments should continue to work with industry to encourage the benefits and mitigate the risks involved in online social networks by jointly establishing industry best practices and guidelines.

Since its early years, the web has undergone a dramatic transformation from largely static webpages to a dynamic, interactive set of web communities. People socialize with their friends on Facebook, Weibo, or Instagram; connect with their colleagues on LinkedIn; explore a virtual world like Second Life; post updates on Twitter; and play games on Xbox Live. Children play on their own social networks like Webkinz or Club Penguin.

The most popular social networks have hundreds of millions of members. Unfortunately, their popularity has also attracted criminals—hackers, spammers, identity thieves, and predators—who misuse the information people disclose to harass, bully, steal identities, and commit fraud. In addition, users of these services may reveal details about their lives that are more lasting and available to a wider audience than they may realize, with consequences for their reputations that they may not imagine. It is essential, therefore, for consumers to understand the risks and take appropriate steps to protect their information, their privacy, and their reputations.

Social networking services raise additional concerns for young people, particularly those under the usual required age of 13, who may use social networks designed for adults. It is important that young people (and their parents and guardians) understand that these sites may contain content inappropriate for children, and that profiles may be viewed by anyone on the Internet. Registering children who are under the required age can violate the terms and conditions of these social sites. Furthermore, young people who are over age 13 but under the age of majority and who lie about their age may bypass protections offered for those under age 18.

Microsoft Approach

Microsoft helps people manage their privacy and safety on social networks through technology tools, education, policies, and partnerships.

CREATING TECHNOLOGY TOOLS

- The Personal Data Dashboard offers a central location for personal information associated with selected Microsoft products and services, and helps you control how it is used by Microsoft. All Microsoft account holders can specify who is able to view their profiles, who can contact them, and who is able to post or view the content they share.
- In Xbox Live, parents can use Online Safety Settings to create individual profiles for each child. This enables them to specify what activities a child can participate in (such as multiplayer gaming, video chat, text messaging, or voice messaging), who they can communicate with, and who can see a child's profile or friends list. In addition, Xbox Live supports a reputation system that rewards healthy participation in games while reducing that of troublemakers and cheaters.

PROVIDING EDUCATION AND ADVICE The Microsoft Safety & Security Center offers guidance on how to use social networks more safely, including those that are location-based, with specific advice for children and teens. Consumers can also find advice on maintaining and restoring their online reputation; suggestions for avoiding online scams; and tips on how to avoid, block, and report inappropriate behavior.

DEVELOPING INTERNAL POLICIES AND practices Microsoft enforces a code of conduct for users of its online services such as Xbox Live, and moderates content and interactions to address illegal activity, inappropriate material, and other abuse.

ESTABLISHING PARTNERSHIPS Creating a safer online environment requires a holistic approach in which government leaders, law enforcement, technology providers, and nongovernmental organizations all play vital roles. Engaging with governments around the world, as well as with organizations like the National Cyber Security Alliance and the Family Online Safety Institute, is central to Microsoft efforts in social networking safety.

Policy Considerations

Policymakers in industry and government can help strengthen the benefits and mitigate the risks involved in online social networks by focusing on these priorities:

- **ESTABLISH AND PROMOTE INDUSTRY BEST PRACTICES** Social networking services should work with governments to establish industry best practices and guidance, such as the Safer Social Networking Principles for the EU.[28] This document "outlines the principles by which social network providers should be guided as they seek to help minimize potential harm to children and young people, and recommends a range of good practice approaches which can help achieve those principles." Microsoft, Facebook, Google, and 15 other technology companies collaborated to develop these principles.

- **PROVIDE FUNDING FOR RESEARCH** Research plays a critical role in identifying the factors that increase risk online and in dispelling myths that can lead to misplaced efforts to address them. Government funding is essential for both academic and industry research in these areas.

- **SUPPORT ONLINE SAFETY EDUCATION IN SCHOOLS** Online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should include modules that teach digital literacy and civility.

28 *Digital Agenda for Europe:* ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

Internet Security at Work

Key Points

- No business is immune to security threats from cybercriminals. However, there are inexpensive practices that companies can implement to better protect the security of their data, workforce, customers, and networks.
- To help companies work more securely on the Internet and protect company data and financial assets against cyber-crime, Microsoft develops technology tools; provides education and guidance; and partners with government, industry, law enforcement, and nonprofit organizations.
- Governments should work with the private sector to strengthen the security, privacy, and reliability of the cyber-ecosystem. In partnership with the private sector, policymakers should build on industry best practices for risk-based, technology-neutral approaches to mitigating cyberthreats.

No business demographic is immune from cyberattacks. High-profile data breaches of major corporations make big news, giving the impression that cybercriminals are interested in targeting only larger companies. However, according to Symantec, in 2012, attacks directed against businesses with fewer than 250 employees showed the greatest increase.[29]

Financially motivated cybercriminals threaten company intellectual property and bank accounts as well as customer or employee data. Thieves may steal employee credentials to initiate transfers from company bank accounts or take customer data, install malware that appropriates or destroys data, or spy on employees for sensitive data, such as passwords. These can be serious threats because successful crimes could destroy an entire business.

Cybercriminals have many avenues to gain access. They may hack weak passwords, exploit vulnerabilities in software and hardware, break in through a stolen laptop, embed malware on a carelessly used flash drive, or infiltrate through an unsecured wireless network or a device used at a mobile hotspot.

They may also use social engineering tactics like spear phishing. Spear phishers carefully research their marks and send email that appears to come from someone within the company—for example, the head of human resources or a coworker. It may request a user name or password or invite the recipient to click a link, which will install spyware or other malware. Cybercriminals may also break into a company network through inadequately secured personal devices that employees use to access corporate data.

Fortunately, the steps to help defend company assets need not require broad security expertise or great expense. Companies can help protect their assets by taking steps that include the following:

- Setting up a secure system by controlling network access, installing legitimate antimalware software, and keeping software current automatically for all devices (personal and company-owned).
- Protecting business data with regular backups, by encrypting sensitive business information, and through the secure disposal of company equipment.
- Training the workforce to create strong passwords, to be on the alert for scams so as not to be tricked into downloading malware, and to treat all public Wi-Fi networks as a security risk.
- Being prepared by developing security policies, including for personal devices that employees use at work. Businesses also need to be aware of threats outside the business network, and to put practices in place that watch for and correct unexpected payments, data leakage, and other such events.

29 2013 Internet Security Threat Report, Symantec: **www.symantec.com/security_response/publications/threatreport.jsp**

Microsoft Approach

Microsoft seeks to address the problem of online security in the workplace through a combination of technology, education, and collaboration.

DEVELOPING TECHNOLOGY TOOLS Microsoft builds technology to help businesses secure their assets:

WINDOWS UPDATE can be set to automatically download and install updates to Windows as well as to device drivers and other Microsoft software.

MICROSOFT SECURITY ESSENTIALS AND WINDOWS DEFENDER help protect against malware. Microsoft Security Essentials is a free program that provides real-time protection against malware. Windows 8 builds in this protection with Windows Defender (replacing Microsoft Security Essentials).

THE SMARTSCREEN FILTER, a feature in many Microsoft products, helps protect against the installation of malware by warning consumers about potential phishing websites and attacks that use social engineering tactics.

THE MICROSOFT SAFETY SCANNER provides free scanning on demand and helps remove malware.

THE MICROSOFT MALICIOUS SOFTWARE REMOVAL TOOL checks computers using supported versions of Windows for prevalent malware and helps remove any infections it finds.

BITLOCKER DRIVE ENCRYPTION AND ENCRYPTING FILE SYSTEM (EFS) are two data encryption options available to some Windows users. BitLocker Drive Encryption encrypts an entire hard drive, and EFS can be used to encrypt individual files as needed.

WINDOWS INTUNE helps companies manage computers and mobile devices from the cloud, enabling people to use the devices they choose while following corporate policies.

PROVIDING EDUCATION AND GUIDANCE Microsoft created the Internet Security at Work Toolkit expressly to help companies teach their employees how to work more securely online and better defend company, customer, and personal information.

ESTABLISHING PARTNERSHIPS Building greater safety and security requires a holistic approach in which government leaders, law enforcement, technology providers, and nongovernmental organizations work together.

Microsoft collaborates with the National Cyber Security Alliance (NCSA), which helps companies assess their security risks, monitor threats, report cyberattacks, and implement a cybersecurity plan. Microsoft also partners with the US Federal Communications Commission (FCC), Federal Trade Commission (FTC), Department of Homeland Security (DHS), and Chamber of Commerce to build business awareness of their role in keeping their networks and employees safer online.

Policy Considerations

Policymakers in government and industry can help companies work more securely on the Internet and protect company data and financial assets against cybercrime by adhering to the following principles:

- **PROMOTE SECURITY TRAINING FOR EMPLOYEES** Industry must establish voluntary guidelines and best practices for employee security training.

- **BUILD ON EXISTING FRAMEWORKS AND BEST PRACTICES** In partnership with the private sector, policymakers should build on industry best practices for risk-based, technology-neutral approaches to mitigating cyberthreats. When policymakers rely upon tested frameworks, they help ensure that hard-won security gains are maintained and technological innovations are given maximum opportunity to succeed.

- **DEVELOP GLOBALLY HARMONIZED LAWS AND STANDARDS** Conflicting laws can complicate compliance across local, state, provincial, or national borders. The wide variance in rules, regulations, and laws threatens to impede economic progress and stifle innovation. In countries such as the United States with multiple state laws, broad federal preemption must be a part of any comprehensive privacy legislation.

Global Online Safety Partnerships and Initiatives

Key Points

- Creating a safer online environment requires a holistic approach in which consumers, government leaders, technology providers, and nongovernmental organizations collaborate.
- Microsoft efforts have centered on engaging through public policy with governments around the world, with organizations like the National Cyber Security Alliance and the Family Online Safety Institute, and on such online safety initiatives as STOP. THINK. CONNECT.
- Cooperation among all stakeholders—consumers, government, law enforcement agencies, the technology industry, and nonprofit organizations—is one of the most effective means for helping to make the Internet a safer, more secure, and trusted environment.

The Internet may be the landmark invention of this era, offering new ways to work, connect, learn, and play. But, like the real world, the Internet comes with risk. Unfortunately, the digital age has enabled sophisticated new ways of causing harm to people and their property, businesses, and even nation states.

One of the best ways to help protect people online is to make them aware of potential pitfalls and help them develop skills and strategies for avoiding them. This requires a holistic approach in which consumers, government leaders, technology providers, and nongovernmental organizations collaborate.

Microsoft Approach

For decades, Microsoft has invested in consumer awareness about the safer use of technology and the Internet. Microsoft efforts have centered on engaging through public policy with governments around the world, as well as with nongovernmental organizations such as the National Cyber Security Alliance and the Family Online Safety Institute, and on such online safety initiatives as National Cyber Security Awareness Month, Safer Internet Day, and STOP. THINK. CONNECT.

NATIONAL CYBER SECURITY ALLIANCE (NCSA). NCSA is a prime example of a successful partnership that includes the Department of Homeland Security, business, and nonprofit organizations. Microsoft was a founding member, has played a leadership role since NCSA's inception in 2001, and has contributed to the following important NCSA initiatives:

National Cyber Security Awareness Month each October is a program dedicated to raising public awareness of online risks and informing people about how to mitigate them. As a key sponsor and serving on the board, Microsoft contributions have included research, consumer guidance on key online safety and security issues, and participation in special forums and events.

STOP. THINK. CONNECT. is a consumer awareness and education campaign that was launched in October 2010. Its simple message—to stop and think before conducting online activities—reminds people to exercise caution. The campaign, created by an unprecedented coalition of 30 representatives from industry, government and the nonprofit sector, was the result of 16 months of research and testing. It is an important step toward building a unified culture of online safety, similar to public awareness efforts aimed at encouraging seat-belt use and preventing forest fires.

FAMILY ONLINE SAFETY INSTITUTE (FOSI) FOSI is an international nonprofit organization that works to make the online world safer for kids and their families. Microsoft employees have served in a leadership capacity, and the company has participated in its research, events, and special projects to develop innovative solutions and policies in the field of online safety. These efforts include the following:

Support for A Platform for Good, which seeks to promote and encourage digital citizenship among parents, educators, and youth. While recognizing the potential risks, it aims to celebrate technology as a vehicle for opportunity and social change. Microsoft continues to promote the initiative through its blogs and other social media.

Financial support for the Global Resources Information Directory (GRID), a comprehensive directory of online safety information that monitors the efforts of countries around the world to make the Internet safer for their citizens.

Work on the Broadband Responsibility Project to create a checklist for implementing a comprehensive broadband responsibility plan in schools, communities, and states.

SAFER INTERNET DAY Microsoft is a long-standing supporter of Safer Internet Day, a global campaign organized by Insafe and co-founded by the European Union, which promotes more responsible use of online technology and devices. Microsoft helps promote the day, provides supporting research such as the Microsoft Computing Safety Index, and leads and participates in activities that help educate consumers about safer online habits.

Policy Considerations

Policymakers can advance the work of global partnerships and initiatives in making the Internet a safer and trusted environment by focusing on the following:

- **SUPPORT PUBLIC AWARENESS EFFORTS** Governments and companies worldwide should invest jointly in Internet safety by supporting programs aimed at increasing public awareness of Internet risks and guidance to help people avoid them.

- **ENCOURAGE COLLABORATION AND PUBLIC-PRIVATE PARTNERSHIPS** Cooperation among all stakeholders—consumers, government, law enforcement agencies, the technology industry, and nonprofit organizations—is one of the most effective means for helping to make the Internet a safer, more secure, and trusted environment.

- **PROMOTE SELF-REGULATION AND FLEXIBLE LEGISLATION** To better protect people online, industry must regulate itself and government must develop thoughtful legislative frameworks for addressing risk in emerging technology areas. As governments do this, it is essential that they leave room for innovation and flexibility in the process.

- **SUPPORT RESEARCH THROUGH FUNDING** Research plays a critical role in identifying the factors that increase risk online and in dispelling myths that can lead to misplaced efforts to address them. Government funding is essential for both academic and industry research in these areas.

Resources

ONLINE SAFETY

Microsoft Security & Safety Center with online safety guidance: **www.microsoft.com/security**

Online Fraud: Your Guide to Prevention, Detection, and Recovery: **aka.ms/OnlineFraudBooklet**

Microsoft Computing Safety Index (MCSI): **www.microsoft.com/security/resources/mcsi.aspx**

National Cyber Security Alliance: **www.staysafeonline.org**

Family Online Safety Institute (FOSI): **www.fosi.org**

A Platform for Good: **www.aplatformforgood.org**

DIGITAL CITIZENSHIP

Microsoft Digital Citizenship in Action Toolkit: **aka.ms/free_resources**

Fostering Digital Citizenship, Microsoft visual whitepaper: **aka.ms/digitalctz**

Research and curriculum materials promoting digital citizenship: **www.digitalcitizenship.net**

Microsoft Global Online Safety Footprint 2013: **aka.ms/safety_footprint**

Online Safety 3.0: Empowering and Protecting Youth: **aka.ms/Online-Safety30**

The Family Online Safety Institute: **www.fosi.org**

CHILD ONLINE SAFETY

Microsoft Security & Safety Center with age-based guidelines for Internet use:
www.microsoft.com/security

The International Centre of Missing & Exploited Children (ICMEC): **www.icmec.org**

The Family Online Safety Institute: **www.fosi.org**

A Platform for Good: **www.aplatformforgood.org**

A comprehensive directory of parental control tools and safety education guidance:
www.getnetwise.org

ONLINE SAFETY EDUCATION

Fostering Digital Citizenship: **aka.ms/digitalctz**

ThinkUKnow: **www.thinkuknow.co.uk**

Microsoft Global Online Safety Footprint 2013: **aka.ms/safety_footprint**

Microsoft Partners in Learning: **www.pil-network.com**

Microsoft YouthSpark: **aka.ms/youthspark**

European Commission Safer Internet Programme: **aka.ms/EC-SaferInternet**

The Microsoft Safety & Security Center with age-based guidelines for Internet use:
www.microsoft.com/security

Microsoft Digital Citizenship in Action Toolkit: **aka.ms/DC-Toolkit**

National Cyber Security Alliance safety tools and materials:
www.staysafeonline.org/teach-online-safety

FAMILY SAFETY SETTINGS

Microsoft Security & Safety Center safety guidelines for the whole family:
www.microsoft.com/security/family-safety

Comparison of Microsoft family safety tools: **aka.ms/compare-tools**

A Platform for Good: **www.aplatformforgood.org**

A comprehensive directory of parental control tools and safety education:
www.getnetwise.org

MICROSOFT COMPUTING SAFETY INDEX

Microsoft Computing Safety Index (MCSI): **www.microsoft.com/security/resources/mcsi.aspx**

The MCSI survey (abbreviated version): **aka.ms/MCSISurvey**

Online safety research from Microsoft: **www.microsoft.com/security/resources/research-studies.aspx**

COMBATING CHILD EXPLOITATION ONLINE

Microsoft PhotoDNA: **www.microsoftphotodna.com**

The Microsoft Digital Crimes Unit: **www.microsoft.com/DCU**

Microsoft Cybercrime Center: **aka.ms/cybercrime-center**

Thorn: Digital Defenders of Children: **www.wearethorn.org**

Microsoft human rights statement: **aka.ms/Human-Rights-Statement**

The National Center for Missing & Exploited Children (NCMEC): **www.ncmec.org**

Microsoft research initiative on the role of technology in human trafficking:
aka.ms/human-trafficking-rfp

COMBATING CHILD GROOMING ONLINE

Microsoft PhotoDNA: **www.microsoftphotodna.com**

The Microsoft Digital Crimes Unit: **www.microsoft.com/DCU**

Microsoft human rights statement: **aka.ms/Human-Rights-Statement**

The National Center for Missing & Exploited Children: **www.ncmec.org**

COMBATING HUMAN TRAFFICKING ONLINE

Microsoft Technology and Human Rights Center: **aka.ms/Technology_Human_Rights**

Microsoft human rights statement: **aka.ms/Human-Rights-Statement**

Global Business Coalition Against Trafficking: **www.gbcat.org**

Polaris Project: **www.polarisproject.org**

International Centre for Missing and Exploited Children (ICMEC): **www.icmec.org**

Thorn: Digital Defenders of Children: **www.wearethorn.org**

Microsoft Research: **research.microsoft.com**

Microsoft PhotoDNA: **www.microsoftphotodna.com**

Microsoft research initiative on the role of technology in human trafficking: **aka.ms/human-trafficking-rfp**

COMBATING ONLINE BULLYING

Microsoft Safety & Security Center materials to help adults and young people stand up to online bullying: **www.microsoft.com/security/family-safety/online-bullying.aspx**

A comprehensive directory of parental control tools and safety education: **www.getnetwise.org**

Cyberbullying Research Center: **www.cyberbullying.us**

An online safety education site that Microsoft created in cooperation with the European Union: **www.saferinternet.org**

Resources to help address bullying in the United Kingdom: www.bullying.co.uk

Wired Safety: **www.wiredsafety.org**

COMBATING ONLINE FRAUD

Online Fraud: Your Guide to Prevention, Detection, and Recovery: **aka.ms/OnlineFraudBooklet**

The Microsoft Digital Crimes Unit: **www.microsoft.com/dcu**

Microsoft Cybercrime Center: **aka.ms/cybercrime-center**

Malicious Software Removal Tool: **aka.ms/msrt**

Microsoft Safety Scanner: **aka.ms/scanner**

The Microsoft Safety & Security Center with antifraud guidance for consumers: **www.microsoft.com/security/online-privacy**

SAFER ONLINE GAMING

The Xbox Live Code of Conduct: **aka.ms/XboxLive_COC**

Family Safety on the Microsoft Safety & Security Center: **www.microsoft.com/security**

Xbox Live Healthy Gaming Guide: **www.xbox.com/en-US/live/healthygamingguide**

Entertainment Software Ratings Board: **www.esrb.org**

Pan European Game Information: **www.pegi.info**

Computer Entertainment Rating Organization: **www.cero.gr.jp**

ONLINE REPUTATION

Microsoft Services Agreement: **aka.ms/services-agreement**

Microsoft Privacy Settings: **www.microsoft.com/security/online-privacy/overview.aspx**

Microsoft Personal Data Dashboard: **aka.ms/dashboard**

Microsoft Safety & Security Center: Take charge of your online reputation: **aka.ms/reputation**

ONLINE SAFETY FOR MOBILE DEVICES

Microsoft Security & Safety Center with mobile safety advice: **www.microsoft.com/security**

Microsoft advice on safer use of location-based services: **aka.ms/location_safety**

Privacy and location services on Windows Phone: **aka.ms/location-privacy**

CTIA–The Wireless Association: **www.ctia.org**

GSM Association: **www.gsma.com**

Coalition of mobile providers in the United Kingdom promoting social responsibility in the mobile phone industry: **www.mobilebroadbandgroup.com**

SAFER SOCIAL NETWORKING

The Microsoft Safety & Security Center guidance: **www.microsoft.com/security**

National Cyber Security Alliance: **www.staysafeonline.org**

The Family Online Safety Institute: **www.fosi.org**

STOP. THINK. CONNECT. Online safety tips and advice: **www.stopthinkconnect.org**

INTERNET SECURITY AT WORK

Internet Security at Work Toolkit: **www.microsoft.com/security/resources/teach-others-work.aspx**

Microsoft guidance for defending computers: **www.microsoft.com/security/pypc.aspx**

FCC Small Biz Cyber Planner 2.0: **www.fcc.gov/cyberplanner**

U.S. Department of Homeland Security Cybersecurity: **www.dhs.gov/topic/cybersecurity**

National Cyber Security Alliance: **www.staysafeonline.org/business-safe-online**

U.S. Chamber of Commerce Internet Security Essentials for Business 2.0: **aka.ms/USCC_biz_security**

GLOBAL ONLINE SAFETY PARTNERSHIPS AND INITIATIVES

Microsoft Safety & Security Center: **www.microsoft.com/security**

National Cyber Security Alliance: **www.staysafeonline.org**

National Cyber Security Awareness Month: **www.staysafeonline.org/ncsam**

Safer Internet Day: **www.microsoft.com/security/resources/sid.aspx**

STOP. THINK. CONNECT.: **www.stopthinkconnect.org**

Family Online Safety Institute: **www.fosi.org**

A Platform for Good: **www.aplatformforgood.org**

Global Resources Information Directory (GRID): **www.fosigrid.org**

Microsoft Computing Safety Index: **www.microsoft.com/security/resources/mcsi.aspx**