

# Trustworthy Computing



## Personal Safety in the Cloud

*Enabling Trusted Interactions and  
Minimizing Risks in the Online World*

February 2011

This document is provided "as is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using the document.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal reference purposes. You may not modify it without written consent from Microsoft.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

All rights reserved.

# Contents

- Executive Summary.....1
- The Cloud: New Opportunities, New Challenges.....2
- Promoting Safer User Interaction and Content .....3
  - Safety Education and Guidance.....4
  - Family Safety Technologies.....5
- Protecting Children from Online Exploitation .....7
- Combating Online Fraud and Scams .....8
- Policy Considerations for Online Safety .....10
- Conclusion.....11

## **Executive Summary**

The emergence of powerful new Internet-connected devices combined with the maturation of high-speed broadband networks and datacenters has provided individuals and organizations with anytime access to a wealth of choices in online applications, services, and data storage. This new era of “cloud computing” offers many benefits, including lower IT costs and greater flexibility for businesses as well as new and easier ways for individuals to connect, share common interests, and access information.

As the volume of content and interactions enabled by cloud computing has grown, the potential for users to encounter objectionable material or face other online risks has increased. However, the fundamental principles, practices, and tools that have evolved over the past two decades to help protect users on the Internet remain effective in the cloud computing realm.

Protecting individuals—especially children—has been a priority for Microsoft since the company began delivering services online in 1994. Today, we work to promote greater online trust and safety through a range of measures. We incorporate online safety features and tools into our products and services. Our internal business policies and practices support safer and more responsible Internet use. We work with organizations worldwide to educate consumers about online risks and how to avoid them. We support law enforcement in investigating and prosecuting cybercriminals. And we collaborate with policymakers on a range of issues associated with online safety.

In light of growing public awareness about online safety and interest in cloud computing, Microsoft has prepared this paper to examine the issues involved and offer an overview of the company’s online safety efforts. This paper also identifies a number of ways that policymakers can help protect individuals online, including enacting stronger laws against cybercrime and child exploitation, supporting industry self-regulatory principles, promoting Internet safety education in schools, and funding research on online risks.

## **The Cloud: New Opportunities, New Challenges**

In recent years, we've seen explosive growth in cloud computing—the use of PCs, mobile devices, and servers to connect seamlessly with applications, services, and data hosted in large, offsite datacenters.<sup>1</sup> In addition to significantly lowering IT costs and increasing flexibility for businesses, cloud-based services and applications are leading people to spend more time online. Social networking sites and instant messaging services keep teens and adults in contact with friends and family and allow them to connect with people who share their interests. Blogs, wikis, e-commerce sites, search engines, and a growing universe of other cloud-based offerings are making content more accessible and the exchange of information more convenient.

This rapidly evolving online world can be a fascinating place to investigate. But just as exploring the streets of a large, unfamiliar city might lead visitors into a rough neighborhood, cruising the Internet without appropriate safeguards can expose users to risks. Since its inception, the Internet has attracted cybercriminals intent on exploiting unsuspecting users. As more individuals, especially young people, tap into the rich opportunities of the cloud, it is important that technology tools and educational resources be available to help them deal with—and avoid—inappropriate content, attempts by cybercriminals to access their personal data, and online bullying.

Although the scope and nature of online threats continue to evolve, the fundamentals of safe and responsible Internet use that have been developed over the past two decades still apply. Microsoft believes that protecting individuals' personal safety in the cloud can be achieved by refining and extending existing educational resources, technology tools, operational policies, legislative approaches, and law enforcement practices.

Since introducing our first online service, the MSN<sup>®</sup> network, in 1994, we have invested significantly in addressing online safety issues as part of our internal business practices. Companywide policies, standards, and procedures ensure that online safety is a top priority in the development of all Microsoft products and services that connect with the web. These measures include enforcing a code of conduct for users of Microsoft online services and moderating content and interactions in those services to quickly address issues such as abuse, illegal activity, and inappropriate material. Microsoft cloud services have built-in tools for users to report abuses; such reports are promptly investigated by our experienced online safety agents.

In our view, creating a safer online environment and strengthening users' trust in the cloud requires a holistic approach in which consumers, government leaders, technology providers, and nongovernmental organizations (NGOs) all play a vital role. In addition to providing online safety tools and features, Microsoft works with public- and private-sector partners worldwide to teach individuals to recognize and minimize online risks. We provide software and training to assist law enforcement in the apprehension and prosecution of criminals who use the Internet to perpetrate scams or traffic in child pornography. We also provide input to government leaders who are responsible for crafting legislation and policies that protect legitimate Internet users and crack down on online abuses.

---

<sup>1</sup> For more information about Microsoft's cloud computing strategy, visit [www.microsoft.com/cloud](http://www.microsoft.com/cloud).

Our efforts are focused in the following areas:

- Enabling people to more safely interact and share information online
- Helping adults manage the use of technology by children and protect them from inappropriate content and contact
- Partnering with law enforcement, industry, and civic organizations to halt the spread of child abuse images and related forms of computer-facilitated child exploitation
- Combating online crimes such as identity theft, phishing,<sup>2</sup> and fraud

## **Promoting Safer User Interaction and Content**

Today, parents face new challenges in monitoring the content their children encounter online, the people they meet there, and what they share in the cloud. With more to explore in the cloud and with kids spending more time online, the odds are greater that young people will see unsuitable material, encounter someone who might try to harm them, or inappropriately expose personal details.

Growth in the use of mobile phones and other Internet-connected devices is also creating the potential for more personal information to be exposed online. This includes data about people's location, which can be transmitted through global positioning systems or Wi-Fi network mapping technologies built into many devices and applications. While geolocation software and location-based services can provide valuable benefits, such as enabling parents to know their children's whereabouts, the potential abuse of this data for stalking and harassment is a cause for concern.

A December 2010 survey by Microsoft in Canada, Germany, Japan, the United States, and the United Kingdom revealed that while many consumers see value in location-based services, the majority also worry about potential misuse of their information. About 40 percent of respondents said they are most likely to use such services to find people in an emergency. However, 84 percent expressed concern about having their location shared without their consent or having their identity stolen through such a service. Other top concerns include loss of privacy and the potential use of location-based services for stalking or online harassment (also known as cyberbullying).

Although these findings indicate that people are more concerned about privacy and protection of their online data than about personal safety with regard to location-based services, both sets of issues clearly need to be addressed by the providers of these services—particularly in the context of how young people use the technologies.

Children may be skilled in technology use, but they do not always recognize the risks associated with the Internet. For the same reason that kids are taught to look both ways before crossing the street, they need guidance in how to set appropriate boundaries, protect themselves and their online identities, and guard

---

<sup>2</sup> Phishing is the use of email, instant messaging, or other electronic communications to trick people into disclosing private information such as passwords and Social Security, credit card, or bank account numbers. Phishing scams often involve luring the victim to a fake website built to look and function like that of a trusted company, such as a bank or online merchant.

information on the computers they use when an adult is not sitting beside them. Parents and caregivers are in the best position to supervise children's online activities, choose what is appropriate for them to see and do online, and talk with them about safe and responsible conduct online. A lot of help is available from Microsoft and other organizations that we support.

### **Safety Education and Guidance**

The Microsoft Online Safety website ([www.microsoft.com/protect](http://www.microsoft.com/protect)) provides age-based guidance for Internet use, including tips on how to teach children what is or isn't appropriate for them to view and share online. The site addresses issues such as "sexting" (sending sexually explicit text messages) and cyberbullying, safer social networking, rules for safely using mobile devices, tips for responsible online gaming behavior, and how to avoid, block, and report online predators. It also offers links to information about Microsoft technologies such as Windows Live® Family Safety 2011 and Microsoft® SmartScreen® Filter that are designed to help protect families from online threats.

Because online safety is a global challenge that requires shared responsibility, partnerships are critical in addressing the issues involved. To help pool resources and make a greater impact, Microsoft supports hundreds of family safety educational organizations and outreach programs worldwide. These include Safer Internet Day ([www.saferinternet.org/web/guest/safer-internet-day](http://www.saferinternet.org/web/guest/safer-internet-day)), which is organized each February by the nonprofit group Insafe and co-funded by the European Union. In 2010, more than 500 Safer Internet Day events were held in 65 countries. As part of these events, 650 volunteers from 25 of Microsoft's European subsidiaries helped teach more than 50,000 parents, teachers, and students about Internet safety in cooperation with local partners and NGOs. (Many of Microsoft's other online safety partnerships are highlighted later in this paper.)

## Family Safety Technologies

Parents can apply what they learn about minimizing online risks by using safety controls built into a wide range of Microsoft products and services. For example, Windows Live Family Safety 2011 provides tools for monitoring and protecting children as they engage in social networking, online search, and general web browsing. (See the related sidebar below.) Windows Live Family Safety complements other parental controls built into the Windows® operating system that help parents manage how their children use a PC, such as when and for how long they can be logged in, which games they can play, and which programs they can run.

Microsoft enables all Windows Live ID account holders to specify who can view their profile, contact them through Windows Live Messenger and Hotmail®, and post or view comments about their shared photos, files, blog posts, and other content in Windows Live. (More information about Windows Live account controls is available at <http://explore.live.com/windows-live-privacy>.)

### Windows Live Family Safety 2011

Microsoft designed Windows Live Family Safety 2011 to help parents empower their children to explore online while also monitoring and protecting them when needed. These parental controls span three core areas:

- **Safer social networking.** Family Safety can be set to block or restrict access to social networking sites. Parents can also choose to restrict children to sites on an approved list that the parent creates.
- **Safer searching.** Most leading search engines offer features to help families avoid inappropriate content, but they use different mechanisms. To help make these protections simpler to activate, Windows Live Family Safety has safe search features on by default when web filtering is turned on. This capability is supported in search engines provided by Bing, Google, Yahoo!, Ask, Yandex, Virgin Media, and Mail.ru.
- **Safer browsing.** For parents who trust their older children to visit sites responsibly, the Web Filtering menu now includes a new “Warn on adult” content option that allows access to all websites but displays a warning when a site might not be appropriate. If the child chooses to visit that site, Family Safety will notify the parent by email.

Other Windows Live Family Safety 2011 features include a new filter that blocks adult content in images, faster browsing and page loading when the web filter is on, and the ability to block paid advertisements on Windows Live websites when a child is logged in using his or her Windows Live ID. (More information is available at <http://explore.live.com/windows-live-family-safety?os=other>.)

#### Web Filtering for Jimmy

Turn on web filtering     Turn off web filtering (activity reports will still be provided)

**Allow list only:** Only allows websites that a parent has added to the Allow list.

**Child-friendly:** Also allows websites in the child-friendly category. Blocks adult sites.

**General Interest:** Also allows websites that are of general interest. Still blocks adult sites.

**Online communication (basic):** Also allows social networking, web chat and web mail. Still blocks adult sites.

**Warn on adult:** New! Allows all websites but warns when the sites contain suspected adult content.

*When the web filter is on, SafeSearch will be locked on in Bing, Google, Yahoo! and other popular search engines. Adult images will also be blocked.*

Safety features and controls for children's gaming activity are integrated into the Microsoft Xbox 360® game console and Xbox LIVE® online service as well as the new Kinect™ for Xbox 360, a full-body movement sensor that lets users control games, movies, music, and television using gestures and voice commands. (See the related sidebar below.) Microsoft also provides practical guidance for families on how to safely enjoy video games and other online media at the Get Game Smart website ([www.getgamesmart.com](http://www.getgamesmart.com)) and the Xbox® website ([www.xbox.com/en-US/Live/HealthyGamingGuide](http://www.xbox.com/en-US/Live/HealthyGamingGuide)).

To help promote greater safety and privacy in the use of location-based services on mobile devices, Microsoft provides a number of controls in Windows Phone 7 that allow users to manage how and when they share data from their phone. For example, Windows Phone applications cannot gain access to geolocation data unless the user specifically allows them to do so. Applications that use geolocation information must provide an option to disable that access, and Windows Phone users can also choose to turn off location-based services for all applications.

### **Xbox 360 and Kinect Safety Features**

To help promote safer gaming by younger users, the Family Settings tools in the Xbox 360 game console allow parents to limit the use of some functionality. Parents can also configure the console to limit online gaming and communication using Xbox LIVE to approved friends and require parental approval for new friends. It also allows users to report inappropriate use of the service. The Kinect sensor for Xbox 360 includes additional safety and privacy controls.

Xbox 360 Family Settings allow parents to:

- Block or limit sharing of a child's profile information, adding of new friends, receipt of user-generated content, and viewing of mature-rated content
- Specify which games a child can play, based on game rating
- Create Xbox LIVE account settings for a child that will be enforced on any machine the child uses to access his or her account
- Require parental approval of a child's list of online friends
- Specify which types of online communication (text, voice, video) are allowed and with whom

Users can also control the following Kinect-specific experiences:

- Specify whether photos taken by games that use the Kinect device can be uploaded to a website outside of Xbox LIVE
- Turn off the Kinect sensors, including the microphones and camera, when the Xbox console is not being used for a Kinect-enabled game
- Disable face recognition for identifying Kinect players
- Disable Kinect's voice-recognition feature

## Protecting Children from Online Exploitation

Every day, millions of people connect and share content on the web in beneficial and constructive ways. But the Internet has also created new avenues for criminals to exploit young people, such as by distributing child pornography (also known as *child abuse images*) or using social networks, chat rooms, and instant messaging for malicious purposes. The web's high degree of anonymity and the difficulty of investigating online crimes that cross national boundaries or agency jurisdictions can make fighting these crimes especially challenging.

### PhotoDNA Technology for Tracking Child Pornography

Trade in child pornography has risen sharply in the Internet age. Since 2003, NCMEC has reviewed nearly 30 million such images. Quickly identifying copies of a known pornographic image is crucial to stopping its redistribution.

Microsoft researchers teamed with Hany Farid, a digital imaging expert and Dartmouth University professor of computational science, to create a more reliable and efficient way of calculating the distinct characteristics of a digital image to match it with other copies of the same image. The resulting technology, PhotoDNA, can do this even if the digital image has been altered—such as through resizing, saving to another format, or editing.

PhotoDNA debuted in 2009 and is now in use by NCMEC to assign a unique signature, called a *hash*, to each image of child pornography or abuse. The hash data is shared with online service providers to match against photos found on their services and help remove child pornography more quickly.

Microsoft commits extensive resources toward developing technology to combat online child exploitation and supporting the efforts of governments and NGOs in this area. We apply filtering tools and employ more than 100 trained experts to help detect, classify, and report child abuse images transmitted using our online properties such as the Bing™ search engine, Windows Live SkyDrive®, and Hotmail. Among the latest tools for this purpose is an advanced technology called PhotoDNA™, which helps automate and refine the search for child pornography among the billions of photos on the Internet. (See the related sidebar on this page.)

Microsoft reports images of apparent child pornography on its sites to the National Center for Missing & Exploited Children (NCMEC), removes them, and bans the individuals or entities responsible for publishing them from using our services. We also operate an international complaint center where users can report incidents of abuse on Microsoft websites. Our safety experts moderate use of the company's online services and web properties to deal with illegal activity and content that violates the established terms of use—including child pornography, violent images, and hateful messages.<sup>3</sup>

We have also worked with law enforcement agencies in Canada and elsewhere to develop the Child

---

<sup>3</sup> Because this important work requires our trained online safety agents to view highly objectionable material on a daily basis, Microsoft has established a wellness program specifically for these employees. Services include one-to-one counseling, monthly group discussions, and a 24-hour crisis hotline. The program has been instrumental in helping Microsoft retain a pool of highly dedicated online safety experts and in strengthening our efforts to combat child exploitation.

Exploitation Tracking System (CETS), a software tool that allows investigators to share and analyze information related to criminal acts such as possessing or distributing child pornography, kidnapping, and physical or sexual abuse. CETS is used by hundreds of law enforcement officers in countries around the world, and additional deployments are planned.

In addition, Microsoft has partnered with INTERPOL, the International Centre for Missing & Exploited Children, and other organizations to help train more than 3,200 law enforcement personnel from more than 110 countries in methods of identifying online child predators, investigating offenses, and assisting victims. To supplement this in-person training, we have also developed a centralized law enforcement portal that provides training, tips, and tools for investigators and information on cybercrime. We released a new and updated version of the portal in December 2010; it currently has more than 1,400 active users and processes more than 400 requests for assistance each year.

## **Combating Online Fraud and Scams**

The Internet has long been a magnet for criminal activity aimed at misleading users into sharing personal information, credit card and bank account numbers, and secret passwords. Using this data, criminals worldwide steal billions of dollars annually from individuals, financial institutions, and online merchants. As greater amounts of personal data are stored and shared online, users of all ages are more susceptible to fraud, deceptive messages, and other threats.

Online scams are increasingly being perpetrated through social networking services such as Facebook and Twitter. For example, cyberthieves have sent messages to social media users offering seemingly useful applications—such as a way to see who has viewed their social profile—that instead place malicious code on the user’s computer and intercept personal information. Other scam tactics include posting a comment on the user’s page that contains a link to a phishing site or a malware download.

The Microsoft Online Safety website ([www.microsoft.com/protect](http://www.microsoft.com/protect)) provides information to help people avoid these types of scams. And Microsoft Security Essentials ([www.microsoft.com/securityessentials](http://www.microsoft.com/securityessentials)) is a free download that provides real-time protection against viruses, spyware,<sup>4</sup> and other malicious software.

The SmartScreen Filter technology built into our Internet Explorer® web browser, Windows Live Hotmail, and Windows Live Messenger helps detect phishing websites and links. When the filter encounters a suspected phishing site, it displays a warning that says “This website has been reported as unsafe” and prompts users to return to their home page to resume safe browsing. The SmartScreen Filter also provides a simple way for users to report suspected phishing websites to Microsoft for analysis, thereby improving the filter’s effectiveness over time.

Another growing safety threat in the cloud is account hijacking, in which identity thieves steal the passwords of legitimate user accounts and then exploit those accounts to send spam or phishing messages. Hijackers have

---

<sup>4</sup> Spyware is software that can be installed on a computer to collect information about users without their knowledge. Cyberthieves often use personal or financial data collected through spyware to commit identity theft, fraud, and other illegal acts.

also been known to exploit social networking accounts and online gamer profiles in order to harass people or trick them into divulging account details. Microsoft is helping to combat this problem through legal action against hijackers and by purging hijacked accounts from our services. We have also built new features into Hotmail that help hijacking victims regain control of their accounts and make it harder for hijackers to compromise an account.

For example, users who are at a public computer and don't want to risk having their true Hotmail password intercepted can request that a single-use code be sent to their cell phone for logging in to the service. Microsoft has also created two new ways that Hotmail users whose accounts have been hijacked can prove that they are the legitimate owner. A "trusted PC" option lets users link their account with one or more of their personal computers. If they get locked out and need to regain control of their account by resetting the password, Hotmail will allow them to do so as long as the request comes from a PC associated with the account. Alternatively, users can arrange for Hotmail to text a secret code to their cell phone that they can use to reset their account password.

Hotmail also proactively detects and locks down compromised accounts when the service identifies significant changes in an account's email volume or finds that spam is being sent from the account. It also checks for suspicious activity, such as logins made from two continents on the same day.

Another Microsoft technology developed for law enforcement agencies, the Computer Online Forensic Evidence Extractor (COFEE), uses digital forensic tools to help investigators—including those with limited technical expertise—gather evidence of live computer activity at the scene of a crime. For example, computer files and activity logs retrieved using COFEE have helped law enforcement agencies to build stronger cases against suspected spammers, identity thieves, child pornographers, and other cybercriminals. We are working with the National White Collar Crime Center and INTERPOL to make the COFEE tool available free of charge to law enforcement investigators in 187 countries.

As part of our efforts to thwart cybercriminals and help legitimate users more easily determine whom to trust online, Microsoft is also developing stronger digital identity verification technologies and protocols and collaborating with others to generate ideas for advancing trust. For more details about this work, please visit [www.microsoft.com/mscorp/twc/endtoendtrust/default.aspx](http://www.microsoft.com/mscorp/twc/endtoendtrust/default.aspx).

## Policy Considerations for Online Safety

While many aspects of personal online safety hinge on users being well informed about the risks and technology providers providing stronger protections in their products, governments also play an important role. In addition to passing stronger laws and increasing resources to help stop criminals who use the Internet to harm children and others, government leaders are uniquely positioned to focus greater attention on online safety as a societal imperative.

Our recommendations to government policymakers include:

- **Strengthen online safety laws.** Many jurisdictions have no laws that define child pornography or punish criminals for possessing or distributing child abuse images. Microsoft works with ICMEC, INTERPOL, and other organizations to encourage governments to enact and strengthen laws in this area. Specifically, we believe that effective legislation must distinguish between adult pornography and child pornography; apply to pornographic images of anyone under age 18; criminalize possession of child pornography, even for personal use; and require Internet service providers (ISPs) to report suspected child pornography. Microsoft is also working with governments and multilateral organizations worldwide, including the Council of Europe and the International Telecommunication Union, to strengthen and broaden cybercrime laws.
- **Support industry self-regulation as well as legislative frameworks in emerging technology areas.** As governments act to address risks associated with emerging technologies and online services, it is important that they not stifle innovation and technology adoption in the process. Government and industry can work together to establish safety principles and provide the means for service providers to self-declare how they will fulfill those principles and transparently demonstrate their progress. Examples include the Safer Social Networking Principles for the European Union and ISP “codes of practice” in the U.K., the U.S., and Australia. Compliance with the U.S. Children’s Online Privacy Protection Act (COPPA) is also based on self-regulation and adherence to both the spirit and the letter of the law.
- **Promote integration of Internet safety education into school curricula and teacher training.** Microsoft believes that students and teachers can benefit from learning to avoid online dangers, protect their family computers, and conduct themselves ethically on the web. We encourage governments to partner with Internet technology providers, online safety organizations, and school districts to help fill this need using a range of available online safety curricula.
- **Commission studies and fund research to advance Internet safety.** Parents, educators, policymakers, and business leaders need up-to-date information about the rapidly changing web landscape in order to better protect children and enhance security, privacy, and safety. Research is particularly important for identifying factors that increase online risks and for dispelling myths that can lead to misplaced efforts. Government funding for both academic and industry research in these areas is essential.

- **Support community events that promote Internet safety.** Governments can help educate children and adults about safer, more responsible Internet use by facilitating local events that present these topics in an engaging format. Examples include school assemblies, community seminars, business leader forums, youth summits, town halls, constituent mailings, and roundtable discussions.

### Resources for Safer Internet Use

Microsoft is working with organizations around the world to develop online safety websites and other resources, including:

- **Internet Keep Safe Coalition** ([www.ikeepsafe.org](http://www.ikeepsafe.org)), a partnership of governors, attorneys general, public health and educational professionals, law enforcement, and industry leaders working together for the health and safety of youth online
- **Family Online Safety Institute** ([www.fosi.org](http://www.fosi.org)), an international nonprofit organization working to develop a safer Internet through education, public policy, education, and events
- **Childnet International** (<http://childnet-int.org/kia>), a UK-based charity that helps educate teachers, parents, and young people about safe and positive use of the Internet through resources such as the Know IT All for Parents guide
- **Pan European Game Information** ([www.pegi.info](http://www.pegi.info)), an age-based rating system designed to help European consumers make informed decisions about which computer games are appropriate for children
- **Netsmartz** ([www.netsmartz.org](http://www.netsmartz.org)), an interactive educational program of the National Center for Missing & Exploited Children (NCMEC) that provides age-appropriate resources to help teach children how to be safer online and offline
- **GetNetWise** ([www.getnetwise.org](http://www.getnetwise.org)), a project of the Internet Education Foundation to highlight the latest web safety issues and teach users how to steer clear of threats
- **OnGuard Online** ([www.onguardonline.gov](http://www.onguardonline.gov)), a U.S. Federal Trade Commission website offering consumer tips, articles, videos, and interactive activities
- **Stop. Think. Connect.** (<http://safetyandsecuritymessaging.org>), an online safety campaign that promotes awareness and safer behavior on the web
- **PédaGoJeux** ([www.pedagojeux.fr](http://www.pedagojeux.fr)), an educational website based in France that promotes online gaming safety

## Conclusion

As advances in devices and cloud computing deliver more powerful capabilities for interacting and sharing information on the web, technology providers, governments, law enforcement, community organizations, and Internet users have a shared responsibility to promote a safer online environment.

Microsoft takes a comprehensive approach to online safety that includes the development of family safety technologies, strong governance policies, responsible monitoring of our online services, guidance and education for families and children, and partnerships to help combat online crime. These efforts align directly with Microsoft's overall commitment to promoting greater trust online and to building products and services that enhance consumer safety.