

# 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 cyber criminals, online bullies, and malicious software.
- Microsoft's approach to online safety includes technology tools; education and guidance; and partnerships with government, industry, law enforcement, and other key organizations to help create safer, more trusted computing experiences.
- Online safety is a shared responsibility, and government and industry should work together to support this objective. Technology companies, governments, businesses, and consumers can partner to innovate, develop, and deploy effective solutions.

## BACKGROUND

The Internet has revolutionized the ways that consumers work, learn, communicate, and play. At the same time, the Internet has also created new risks and 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; identity theft by criminals; and unwanted contact from spammers and other individuals with malicious intentions.

Consumers are concerned about these risks and are taking steps to protect themselves. A Microsoft research report<sup>1</sup> released in 2011 found that 90 percent of adults and youth in the United States and four European countries have taken some steps to manage their online profiles. However, only 44 percent of adults and youth reported actively thinking about the long-term consequences that their online activities may have on their reputations and identities.

While consumers are actively working to protect themselves, they also have high expectations that industry and government will work to make the online world more secure. If companies fail to meet these expectations, consumers will be less inclined to use online technologies, and both industry and individuals will suffer from a lack of trust.

The unique challenges of online safety require a coordinated response. Technology companies, governments, businesses, and consumers must work together to innovate, develop, and deploy effective solutions. Technology companies must be committed to creating a safer and more trusted Internet. Sensitive data and personal information must be protected, and technology should facilitate business practices that promote trust. Microsoft believes that addressing these present and future challenges requires the collaborative efforts of technology companies, governments, consumers, and businesses.

---

<sup>1</sup> *Teen Online Reputation: 13-17 Years Old*  
[www.microsoft.com/security/resources/research.aspx#teen](http://www.microsoft.com/security/resources/research.aspx#teen)

## MICROSOFT APPROACH

Microsoft takes a three-pronged approach to helping create safer, more trusted computing experiences.

- **Technology tools.** Microsoft offers a number of online safety tools, including Microsoft Security Essentials, a free antimalware program. Microsoft enables all Microsoft account holders to specify who can view their profiles, who can contact them, and who can post or view the content they share. Microsoft Family Safety provides tools that help parents monitor and protect children online, and Xbox 360 comes equipped with Console Safety Settings.
- **Education and guidance.** The Microsoft Safety & Security Center provides guidance for safer Internet use. It offers tips and advice on how people can better secure their computers, protect their online reputations, avoid online scams, help secure their mobile devices, and avoid, block, and report inappropriate behavior.
- **Partnerships.** Creating a safer and more trusted online environment requires a holistic approach in which consumers, government leaders, technology providers, and non-governmental organizations (NGOs) all play a vital role. Central to Microsoft's focus is engaging, through public policy, with governments around the world and with NGOs such as the National Cyber Security Alliance.

## POLICY CONSIDERATIONS

- **Support public and private partnerships.** Microsoft believes public and private partnerships are essential to address the increasing complexities of cyber crime. The company works with law enforcement agencies by providing them with technical training and by developing new technology tools to combat cyber crime. Microsoft also helps protect consumers through legal action to stop cyber criminals, including actions to shut down botnets, and by bringing legal action against the purveyors of fake security software. Other efforts involve developing and sharing PhotoDNA, a technology that helps industry and government find and remove some of the worst images of child sexual exploitation from the Internet.
- **Support industry self-regulation and legislative frameworks.** As governments address the risks associated with emerging technologies and online services, it is important that they foster an environment of technological innovation in the process. Government and industry can work together to establish safety principles and allow service providers to help fulfill those promises. Examples include the Safer Social Networking Principles for the European Union and an ISP code of practice in Australia.
- **Commission studies and fund research to advance Internet safety.** Research plays a critical role in identifying factors that increase online risks and in dispelling myths that can lead to misplaced efforts. Government funding is essential for both academic and industry research in these areas.
- **Online safety education in schools.** Microsoft believes that online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should include modules focusing on online safety, online security, and online ethics.



## Helpful Resources

Microsoft Security & Safety Center with online safety guidance

[www.microsoft.com/security](http://www.microsoft.com/security)

*Online Fraud: Your Guide to Prevention, Detection, and Recovery*

[aka.ms/OnlineFraudBooklet](http://aka.ms/OnlineFraudBooklet)

Security tips and advice from the National Cyber Security Alliance

[www.staysafeonline.org/](http://www.staysafeonline.org/)