Safer Social Networking

Key Points

- Social networks are very popular and offer enriching experiences, but they may include risks such as exposure to malicious software, potential loss of privacy, harassment, online bullying, and damage to reputation.

- Microsoft's approach to making social networks safer includes technology tools; education and guidance; internal policies and practices for moderating content and addressing online abuses; and partnerships with government, the technology industry, law enforcement, 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.

BACKGROUND

In recent years, the web has undergone a dramatic transformation from largely static webpages to a dynamic, interactive set of web-culture communities. There, people connect with their friends on Facebook or Pinterest or colleagues on LinkedIn, explore a virtual world like Second Life, post updates on Twitter, or 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 help protect themselves—their information, their privacy, and their reputations.

Social networking services may 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 many profiles can 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 over 13 but under the age of majority who lie about their age may bypass protections offered for those under 18.

MICROSOFT APPROACH

Microsoft's approach to helping create safer, more trusted digital world includes:

- **Technology tools.** Microsoft offers a number of online safety tools, including Microsoft Security Essentials, a free antimalware program, and the Microsoft Personal Data Dashboard. The Dashboard offers a central location for personal information associated with selected Microsoft products and services to help customers control how their information is displayed.

  Also, Microsoft has built family safety features into many of its products, including Microsoft Family Safety in Windows 8, which helps monitor and protect children online, Kid's Corner on Windows Phone, and Console Safety Settings for Xbox and Xbox 360.

- **Education and guidance.** 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.

- **Internal policies and practices.** Microsoft enforces policies such as a code of conduct for users of Microsoft online services, and moderates content and interactions to address illegal activity, inappropriate material, and other abuse.

- **Partnerships.** Creating a safer online environment requires a holistic approach in which government leaders, law enforcement, technology providers, and non-governmental organizations (NGOs) all play vital roles. Central to Microsoft's efforts is engaging, through public policy, with governments around the world and with NGOs such as the National Cyber Security Alliance and the Family Online Safety Institute.

POLICY CONSIDERATIONS

- **Support public and private partnerships.** Social networking services should work with governments to help protect their customers by establishing industry best practices and guidance, such as the *Safer Social Networking Principles for the EU*.[1] This document "outlines the principles by which social network providers should be guided as they seek to help minimise 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 social networking services collaborated to develop these principles.

- **Commission studies and fund research.** Research plays a critical role in identifying the factors that increase risks to people 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.

- **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 that teach cyber safety, cyber security, and cyber ethics.

[1] **ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf**

Helpful Resources

The Microsoft Safety & Security Center safety 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