February 2013

Microsoft Computing Safety Index

Key Points

- The Microsoft Computing Safety Index (MCSI) is a tool developed as the result of a multiregional survey to determine the best methods for effectively managing and overcoming threats to security and safety online.
- Microsoft uses the MCSI in annual research 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 Safety & Security Center offers education, guidance, and free tools to help people protect themselves online.
- Microsoft welcomes government support in fighting online security risks, and believes that cooperation with authorities is the most effective way to reduce the impact of cyber threats. Microsoft supports a balanced approach to regulation as part of those efforts.

BACKGROUND

As more people connect online, the need for security, safety, and privacy grows, too. 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.

To that end, the company commissioned a study in 2010 to learn how people protect themselves online. That research laid the foundation for the development of the Microsoft Computing Safety Index (MCSI), which can be used to assess online safety behavior and security tool use. The index rates more than 20 protective steps people can take—the more steps taken, the higher the online safety score, with 100 being the highest rating possible. The index is based on three tiers of safety activity:

- Foundational (30 points) includes steps consumers can take such as ensuring that antivirus software is installed and up to date, and that automatic updates are turned on.
- Technical+ (40 points) includes managing online information, hiding IP addresses, and monitoring privacy settings.
- Behavioral (30 points) includes using strong passwords, visiting reputable sites, and staying informed about late-breaking security and safety issues.

Microsoft commissions annual research using the MCSI to study how consumers protect themselves and their families online. The 2012 study, which surveyed more than 10,000 adults from 20 countries found that more than half (55 percent) of the respondents are experiencing multiple online risks, yet only 16 percent say they take proactive steps to help protect themselves and their data.

The 2012 survey examined safety behaviors on mobile devices. Researchers found that while 42 percent of those surveyed run software updates on their personal computers, only 28 percent run regular updates on their mobile devices. Other important findings of the 2012 MCSI research:

- The two most common computer threats that respondents experienced were fraudulent email messages asking for personal information or announcing the detection of a virus, and actual instances of viruses, bots, adware, or spyware on their computers.
- Of the respondents, 31 percent had installed mobile antivirus programs on their devices and keep them current; 23 percent reviewed their location and privacy settings when using social media.
- Citizens of Singapore (average MCSI score 42), Malaysia (40), Canada (39), and Australia (39) had the highest scores for online safety on a computer.

MICROSOFT APPROACH

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

Technology tools. Microsoft offers many free technology tools to reduce online risk, including Microsoft Security Essentials, a free antimalware program. In addition, 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, and Console Safety Settings for Xbox and Xbox 360.

Security response. The Microsoft Security Response Center employs some of the world's top computer security experts to help Microsoft customers prioritize and manage their responses to cyber threats. When a new threat emerges, the Center's researchers analyze the threat and release security updates to address it.

Policy leadership and collaboration. Microsoft believes that a holistic approach to creating safer online environments requires partnerships with consumers, technology providers, industry, governments, and non-governmental organizations.

POLICY CONSIDERATIONS

- Microsoft believes that cooperation between government and technology industry leaders is the most effective means of reducing cyber threats, and supports balanced regulation as part of that effort. Microsoft believes less onerous industry restrictions will lead to greater innovation and flexibility in responding to cyber crime.
- Microsoft believes in the necessity of working with law enforcement and providing technical training and new technologies to help reduce the impact of cyber crime.
- To improve the overall security of online systems, Microsoft supports government funding for basic security research and welcomes government support for combating cyber threats.
- Microsoft is committed to helping protect consumers by bringing legal action or assisting consumers in their own actions to stop cyber criminals.

Helpful Resources

An abbreviated version of the MCSI survey
aka.ms/MCSISurvey

Microsoft Security Essentials, a free security tool
www.microsoft.com/security_essentials

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