

# National Cyber Security Alliance



## Key Points

- Governments, law enforcement agencies, the technology industry, and nonprofit organizations share the responsibility for helping make the Internet safer and more secure.
- For the past 10 years, the United States has designated October as National Cyber Security Awareness Month (NCSAM), a time to more formally encourage everyone to use the Internet more safely and responsibly.
- Microsoft is a founding member of the National Cyber Security Alliance (NCSA) and a key sponsor of NCSAM, which has expanded beyond the United States to include Canada and several members of the European Union. Microsoft encourages governments worldwide to adopt and promote October as Cyber Security Month as one way to help raise awareness of Internet risks among their people.

## BACKGROUND

Microsoft and others in the technology industry have long maintained that helping to keep individuals and families safer online is a responsibility best shared among industry, government, law enforcement, and nonprofit organizations.

The National Cyber Security Alliance (NCSA) is a prime example of just such a successful partnership between the Department of Homeland Security, business, and nonprofit organizations. Microsoft, a founding member of the NCSA, has played a leadership role since its inception in 2001.

National Cyber Security Awareness Month (NCSAM) in the United States is a project of the NCSA—31 days dedicated to raising public awareness of online risks and informing individuals about ways they can help mitigate those risks. Microsoft contributions have included research, new consumer advice and guidance on key online safety and security issues, and participation in special forums and events.

October 2013 will mark the tenth anniversary of NCSAM and will welcome new signatories—Canada and eight members of the European Union. In 2012, those EU states—the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain, and the United Kingdom—piloted a European Cyber Security Month to great success.

Another significant NCSA contribution and example of public-private collaboration has been its signature consumer awareness and education campaign, STOP. THINK. CONNECT., launched in October 2010. Its simple message—to stop and think before going online—reminds people to exercise caution. The campaign, created by an unprecedented coalition of 30 private companies, nonprofit organizations, and government agencies, was the result of 16 months of research and testing.

## MICROSOFT APPROACH

Microsoft takes a three-pronged approach to improving online safety:

- **Technology tools.** Microsoft offers a number of online safety tools, including Microsoft Security Essentials, a free antimalware program for consumers. Microsoft account holders can specify who can view their profiles, contact them, and post or view comments about their shared content. Microsoft Family Safety provides tools that help monitor and protect children online, and Xbox comes equipped with safety settings.
- **Education and guidance.** The Microsoft Safety & Security Center provides guidance for safer Internet use, including tips on how consumers can secure their computers, protect their online reputations, avoid online scams, secure mobile devices, and avoid, block, and report inappropriate behavior.
- **Building relationships.** Central to Microsoft's focus is engaging, through public policy, with governments around the world and with non-governmental organizations (NGOs) such as the NCSA.

## POLICY CONSIDERATIONS

- Microsoft encourages governments and companies worldwide to invest jointly in Internet safety by supporting programs aimed at increasing public awareness and education. This could include adoption and support of October as Cyber Security Awareness Month, and STOP. THINK. CONNECT. as a central campaign to raise public awareness.
- Microsoft believes that cooperation among all stakeholders is the most effective means for reducing Internet risks, and supports balanced regulation that leaves room for innovation and flexibility in responding to those risks.



## Helpful Resources

Microsoft Safety & Security Center  
[www.microsoft.com/security](http://www.microsoft.com/security)

Microsoft's online safety updates on Facebook  
[www.facebook.com/SaferOnline](http://www.facebook.com/SaferOnline)

National Cyber Security Alliance  
[www.staysafeonline.org](http://www.staysafeonline.org)

STOP. THINK. CONNECT. Online safety tips and guidance  
[www.stopthinkconnect.org](http://www.stopthinkconnect.org)