

Sponsored by:



NETWORKWORLD

This story appeared on Network World at <http://www.networkworld.com/newsletters/sec/2010/060710sec2.html>

Socializing safely via the Internet

[Security Strategies Alert](#) By M. E. Kabay, Network World
June 09, 2010 12:06 AM ET



In my [last column](#), I exhorted readers to contribute to integrating cyberspace into our young people's moral universe by getting out into their communities and speaking about Internet safety and other matters of interest.

Today's column consists of the notes I distributed at the first of four public discussions on such topics at the [Brown Public Library](#) in [Northfield, Vt.](#). In no sense should anyone think of these as comprehensive; they were just talking points that I thought would interest participants for an hour-long discussion. I hope that readers will find them useful enough to share with their families and especially as a basis for discussion with young people.

1. Parents, think carefully about how early you should allow your children to have unsupervised access to the Internet. Putting the family computer in the living room until kids are in their early teens can make a lot of sense to keep children from become involved with content and people you would disapprove of without giving you a chance to talk to them about your values.
2. Think you are anonymous because you use a smart handle like "CleverStudentinVermont?" Think again. You may not sign your name to what you post, but with enough effort by investigators, you can usually be tracked down through the details of your Internet connections.
3. Anything you post or write online may be permanently available to anyone, anytime: so think before you post. Ask yourself the following questions before hitting SEND – and if you answer YES to any of the following, don't post!
 4. Would you be ashamed to have your message / photograph / comment publicized in your hometown newspaper?
 5. Would you be unhappy about having your employer / family / spouse / children / parents reading / looking at what you posted?

Sponsored by:

An advertisement for a report titled "path TO THE CIO". It features a globe graphic on the left and a yellow "Download Now!" button on the right. The text reads: "Not all IT professionals are cut out for the CIO job. Read this report to see how real-world CIOs leveraged their skills and management talents to get to the top." Below the text, it says "BROUGHT TO YOU BY CIO".

6. Are you posting evidence of a illegal activities (e.g., under-age drinking, assault, vandalism)?
7. If you are a young person younger than 18 years of age, try to imagine that your concepts of privacy may change as you get older.
8. If you are younger than 18 years old, sending cute pictures to your friends via cell phone is OK, but that doesn't mean it's a good idea to send pictures of yourself stark naked – that's called [sexting](#) and it is classified as child [pornography](#). Making, storing and transmitting child pornography are all federal felonies – crimes with serious jail time.
9. Online dating has its risks: how do you know that the attractive person on the other end of the instant-messaging session or e-mail link is who (s)he says (s)he is? Or what gender, age, financial situation, and criminal record really apply to "Bobbi?"
10. Never arrange to meet someone in private and alone whom you've known only through the Internet. Always meet in a public place and make sure they know you will bring along a friend and that you are telling other people where you are going and whom you are meeting.
11. Parents and children must be on guard against abuse by pedophiles, who have referred to the Internet as a shopping center for their perversion. Some classic signs of child entrapment by pedophiles:
 12. Establishing an attractive image as a slightly older friend or substitute parent;
 13. Working on making the victim separated from and increasingly hostile towards their own family while increasing dependence on the abuser;
 14. Breaking down conventional limits on sexuality by asking for more and more deviant requests such as increasingly intimate photographs, poses and items; and
 15. Asking for and then demanding an isolated meeting and physical contact.
16. Kids should tell parents at once if any Internet contact tells them to keep their communications secret from the parents.

Anyone interested in using these notes verbatim or with modifications should feel free to do so without having to ask me for permission; I'm delighted to make all my teaching materials freely available to anyone provided that they are neither posted on a public Web site nor sold.

* * *

For further reading:

FBI (2010). "[A Parent's Guide to Internet Safety](#)." US Federal Bureau of Investigation. Also available for download as a PDF file.

Kabay, M. E. (2002). [Cyber-Safety for Everyone: From Kids to Elders](#).

Kline, M. J (2005). "[Internet Socializing: Tips for Elementary School Parents](#)." Human Relations Service, Wellesley Hills, MA.

Wiredsafety.org

[Read more about security](#) in Network World's Security section.

[M. E. Kabay](#), PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of [Adaptive Cyber Security Instruments, Inc.](#) and Associate Professor of [Information Assurance](#) in the [School of Business and Management](#) at [Norwich University](#). Visit his [Web site](#) for white papers and course materials.

All contents copyright 1995-2010 Network World, Inc. <http://www.networkworld.com>