Tip Sheet

Common Sense on Online Security

Just as in real life, it is important that teens know who they can trust with their information online. Entering information into forms and profiles online is part of our lives, but it's not always obvious what's legit and what's fake. Teens should also know that more and more companies are following what they do online, whether it's to create personalized content or sell the information to advertisers.

Here are some of the things that teens need to be aware of:

- Phishing: Phony emails, messages, texts, or links to fake websites that scam artists use to trick people into giving out personal and financial information.
- Clickjacking: Scam artists tricking users to click on a seemingly harmless webpage, usually on a social network site, in an attempt to steal information or spread scams to others.
- Computer Virus: A program that can replicate itself and spread from one computer to another through the Internet, CD, DVD, or USB drive. A virus attaches itself to a program so that each time it runs, the virus does too, causing problems on the computer.
- Spyware: Programs that secretly collect small pieces of information about a computer user without him or her knowing.
- Cookies: Data files stored on computers when people visit certain sites, which companies can use to identify repeat customers and personalize visitors' experiences.
- Targeted Advertising: Ads that are tailored to Internet users based on the information companies have collected about them.

So what can they do to protect themselves?

Common Sense says:

Create strong passwords. A powerful password helps protect accounts. Teens should never share passwords with friends, and they should update their passwords frequently. A great site for creating strong passwords is www.strongpasswordgenerator.com.

Think twice before downloading. Content that teens download from nonsecure sources can plague a computer with spyware and viruses. Encourage teens to only download and install programs if they are familiar with the website and program and have read the end-user license agreement.

Be careful when sharing information. Teens should be cautious when sharing information such as their full name, address, and account numbers. Messages that ask teens to share private information can be red flags for scams. If teens suspect a scam, they should not reply to it and not click on links in the message. Encourage them to report such phishing to your Internet service provider.

See what phishing and clickjacking looks like. It's a great way to understand how to avoid being tricked. Check out the examples at: www.consumerfraudreporting.org.

Install the latest security updates. Your computer can be protected from viruses, spyware, and other security problems by using up-to-date security tools.

Consider limiting data collection. If you have privacy concerns, consider disable Internet "cookies," limiting clicking on ads, and examining a website's privacy policy before revealing any information on it.

Sources
Common Sense Media. "Protecting Our Kids' Privacy in a Digital World." December 2010. <http://www.commonsensemedia.org/privacy.>
Stecklow, S. "On the Web, Children Face Intensive Tracking." The Wall Street Journal. September 17, 2010.

common sense media