For Youth

Common Sense on
Online Security

Just as in real life, the Internet has both trustworthy people and scammers. And it's not always obvious what's legit and what's fake. Now that more and more companies are following what we do online -- whether it's to create personalized content or sell data to advertisers – it's really important to view information critically.

Here are some of the things that you 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 you do to protect yourself?

Common Sense says:

Create strong passwords. A powerful password helps protect your accounts. Never share passwords with friends, and update your passwords frequently. A great site for creating strong passwords is www.strongpasswordgenerator.com.

Think twice before downloading. Content that you download from nonsecure sources can plague a computer with spyware and viruses. Don't download and install programs unless you are familiar with the website and program and have read the end-user license agreement.

Be careful when sharing information. Practice caution when entering information such as your full name, address, and account numbers. Messages that ask you to share private information can be red flags for scams. If you suspect a scam, don't reply and don't click on links in the message. 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 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 disabling 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