common sense media

Mentor Tip Sheet

MIDDLE & HIGH SCHOOL

Online Security

What's the Issue? Just as in real life, it is important that teens know who they can trust with their information on the internet. Entering information such as their name, age, and address into forms and profiles online is common, but teens can be tracked by companies or tricked into scams that put themselves at risk for identity theft. Maybe they are tricked into filling out a form for a fake sweepstakes. Maybe they click on an attachment that installs spyware on their computer. Or maybe they click on ads and enter their email address, which the advertiser can then sell to other companies.

Digital security refers to keeping us, our information, and our digital devices secure from outside threats. These issues affect everyone – teens, families, and even whole online communities. Online security issues can be divided into three categories:

Scams and identity theft. Criminals may try to trick teens into giving out private information. They use this information to attempt identity theft, which can ruin a teen's financial future and make it difficult to make purchases and get loans. Criminals target young people and children because they have cleaner financial records than adults. Risks include:

- 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.

Viruses and spyware. Many teens download and share music, movies, or games. However, teens should only download from secure sites, and avoid clicking on links and attachments that can put themselves at risk. Viruses and spyware can be blocked with security tools. Risks include:

- 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.

Companies tracking users. One of the fastest-growing business strategies is to monitor the information, behavior, and even location of internet users. Companies do this so they can personalize visitors' experiences and sell their information to advertisers. On the downside, most teens don't know that their online activity is being tracked. Companies aren't legally required to share how they track consumers' behaviors, which is often buried in the fine print of their privacy policies. On the upside, it can be nice for teens to have websites tailored to their interests. Issues include:

- 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.

Why Does It Matter?

Teens should understand that when they're online, companies are watching and tracking their behavior, and scam artists might be trying to trick them into giving out information. If teens don't understand digital security risks, their devices can be damaged, they can fall prey to scams, or they can increase their risk of identity theft. It's up to teens to protect themselves so they don't become targets.

What Mentors Can Do

What are the benefits and drawbacks of companies tracking your online information, behavior, and location? When you download from the internet, how do you make sure it's from a secure site? Have you ever encountered a phishing mess?

Create strong passwords. A powerful password does wonders to protect accounts. Teens should never share passwords with friends, and they should update their passwords often. 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 download only from secure sites.

Be careful when sharing information. Teens should be careful when sharing information such as full name, address, and account numbers. Messages that ask teens to share private information are 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 the 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. Help teens take control over their own information by: 1. disabling internet "cookies" so companies cannot track online behavior, 2. limiting clicking on ads, and 3. 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.common sensemedia.org/privacy.>

Stecklow, S. "On the Web, Children Face Intensive Tracking." The Wall Street Journal. September 17, 2010.