



GRADES K-8 STUDENT TIP CARD

In a world driven by technology, students are exposed to electronics and the Internet earlier in life than ever before. From gaming consoles to their own smart phones and tablets, kids have access to multitudes of information but also numerous risks from online threats. By learning safe online habits now, students can make smarter online decisions and teach their friends or parents how to be safer digital citizens for the rest of their lives.

DID YOU KNOW?

- **Seventy-five percent of children are willing to share personal information** online about themselves and their family in exchange for goods and services.¹
- In 2012, **26 percent of identity theft victims** were between the ages of six and 10, and identity theft has doubled in the past year for children age five and younger.²
- **Child identity thieves use their victims' Social Security Numbers** to open credit cards and secure auto loans, student loans, mortgages, and business lines of credit.³
- **Seventeen percent of children** between the ages of 10 and 13 surveyed reported receiving an email or online message with photos or words that made them feel uncomfortable.⁴

SIMPLE TIPS

- Trust your feelings. If something doesn't feel right when you are online, stop what you're doing.
- Think before you click. Don't open emails or download attachments from strangers.
- Talk to a parent, teacher, or trusted adult if something makes you feel uncomfortable.
- Keep your personal information private; avoid sharing your name, address, telephone number, and the name of your school when using the Internet or any apps.
- Just like in real life, treat others like you want to be treated online. Do not bully or say/post things online that could hurt other's feelings or get you in trouble.
- Remember to protect your cell phone and tablet. Use a PIN or password to lock the devices. The same tips for being safer online apply when you access the Internet from any device, like smart phones, video game consoles, etc.

¹ SentryPC, "Children and Teen Statistics", eMarketer, <http://www.sentrypc.com/home/statistics.htm>

² Child Identity Theft Report, 2012

³ Ibid.

⁴ <http://www.guardchild.com/statistics/>, 2013



RESOURCES AVAILABLE TO YOU

NetSmartzKids.org

Clicky, a yellow robot, along with brother-and-sister team Nettie and Webster teach kids what to watch out for online in this interactive website with videos and games.

iKeepSafe.org

Faux Paw, the Websurfing Techno Cat, is always on an adventure. Read about her trip to Beijing or her experiences with the dangerous download.

NSTeens.org

Real-life stories, games, and comics that explore potential online dangers and how to avoid them.

iSafe.org

Become an iMentor and promote cyber safety awareness in your home, school, and community.

IF SOMETHING HAPPENS ONLINE

- Turn off the computer monitor.
- Tell a parent, guardian, teacher, or adult you trust.

www.dhs.gov/stopthinkconnect.

www.dhs.gov/stopthinkconnect



GRADES 9-12 STUDENT TIP CARD

Technology allows students access to more information than ever before. Students now utilize technology for standardized tests, online classes, and college applications. From gaming consoles to their own smart phones and tablets, kids have access to multitudes of information but also numerous risks from online threats. By learning safe online habits now, students can make smarter online decisions with what they decide to share and do online. Students can also teach their friends or parents how to be safer digital citizens for the rest of their lives.

DID YOU KNOW?

- Forty-three percent of teens have been victims of cyberbullying.⁵
- Fifty-two percent of teens who have been victims of cyberbullying do not tell their parents about it.⁶
- Ninety-six percent of teens use social networking applications such as Facebook, MySpace, chat rooms, and blogs.⁷
- One in five U.S. teenagers who regularly log on to the Internet say they have received an unwanted sexual solicitation via the Web.⁸

SIMPLE TIPS

- Keep your personal information private, including the names of your family members, your school, your telephone number, and your address. Turn off your GPS location services and your device's camera when not using them.
- Avoid sharing your whereabouts online to avoid cyberstalking. Wait to post those concert or trip pictures until you get home so criminals are not aware when you aren't home.
- Think twice before you post or say anything online; once it is in cyberspace, it is out there forever. Remember that what you post may impact you getting a job and keeping a job in the future.
- Only do and say things online that you would do or say in real life. Think about how your decisions on what you post or say online can have positive or negative consequences later.
- Speak up. If you see something inappropriate, let the website know and tell an adult you trust. Don't stand for bullying—online or off.
- Use strong passwords with eight characters or more that also use a combination of numbers, letters, and symbols. Don't share your passwords with anyone.

⁵ National Crime Prevention Council, <http://www.ncpc.org/resources/files/pdf/bullying>

⁶ <http://www.guardchild.com/statistics/>, 2013

⁷ <http://www.statisticbrain.com/cyber-bullying-statistics/>, 2013

⁸ ABC News, "One in Five Kids Solicited Online", 2013

- 
- Think before you click—don't open e-mails from strangers and don't click on links for unfamiliar sites.
 - Be careful who you friend online. Simply because someone with mutual friends wants to add you on a website or app does not mean they are trustworthy.
 - Use privacy settings on social networking websites such as Twitter, Instagram, SnapChat, and Facebook.
 - Be cautious when downloading applications on your smartphone—they may contain malware that could infect your device.
 - Be sure to review and understand the details of an app before installing it, and be wary of the information it requests.

RESOURCES AVAILABLE TO YOU

StopBullying.gov

Find out what to do if you or someone you know is being bullied.

Cybersecurity Awareness Volunteer Education Program (C-SAVE)

Access resources for holding a cybersecurity discussion with your peers at www.staysafeonline.org/in-the-classroom/c-save.

NSTeens.org

Watch real-life stories, play games, and read comics that explore potential online dangers and how to avoid them.

iSafe.org

Become an iMentor and promote cyber safety awareness in your home, school, and community.

IF YOU'VE BEEN COMPROMISED

- Talk to a parent, guardian, teacher, or adult you trust.
- Keep all evidence of the interaction and write down the date and time when the incident occurred.
- Contact local law enforcement to file a report.
- If you received an online solicitation, make a report at www.Cybertipline.com or call 1-800-843-5678.
- If you are the victim of online fraud, report it to the Department of Justice at www.justice.gov/criminal/cybercrime/reporting.

www.dhs.gov/stopthinkconnect.

www.dhs.gov/stopthinkconnect



UNDERGRADUATE STUDENT TIP CARD

In countless ways, technology drives our society every day. Students can now apply for jobs and scholarships easily online. Numerous colleges are exclusively online. It's possible to pay bills, online shop, and converse with others all while using a mobile device on the go. Although technology assists us in our fast-paced world, it is important to recognize the risks associated with online use and take important yet simple steps to protecting our information.

DID YOU KNOW?

- In 2012, 31 percent of all identity theft complaints received by the Federal Trade Commission were filed by young adults.⁹
- Thirty-seven percent of employers use social networking sites to research job candidates.¹⁰
- National figures show victims of cyberstalking tend to be females between the ages of 18 and 29 but women are not the only targets.¹¹

SIMPLE TIPS

- Use antivirus software to protect all devices, such as computers, tablets, smartphones, and gaming systems that connect to the Internet; only connect to the Internet over a secure network.
- Avoid sharing your exact whereabouts online to avoid cyberstalking; wait to post those concert or trip pictures until you get home so criminals are not aware when your house is vacant.
- Always use privacy settings on social networking websites, and think twice about what you are posting and saying online. It can affect your ability to get a job later in life. Don't forget that your online friends may include recruiters, adults, siblings, and professors. Set a good example for others in what you share and post online.
- When banking and shopping online, make sure the site is security enabled with "https://" or "shttp://".
- Be wary of messages that implore you to act immediately as well as offers that invite you to join an event or group on a social networking website with incentives like free gift cards.
- If you see something inappropriate online, let the website know so they can take action.

⁹ <http://cencal.bbb.org/article/attention-college-students-43437>, 2013

¹⁰ <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2F18%2F2012&ed=4%2F18%2F2009>, 2012

¹¹ "Cyberstalking and Women - Facts and Statistics", 2014

<http://womensissues.about.com/od/violenceagainstwomen/a/CyberstalkingFS.htm>

- 
- Use strong passwords with eight characters or more that use a combination of numbers, letters, and symbols. Don't share your passwords with anyone.
 - Be careful who you friend. Simply because someone with mutual friends wants to add you on a website or app does not mean they are trustworthy.
 - Be cautious when downloading applications on your smartphone—they may contain malware that could infect your device.
 - Avoid using peer-to-peer file sharing software for music and other downloads; this type of software frequently contains viruses or malware and can expose sensitive information stored on your computer to others using the software.
 - Review and understand the details of an app before installing it, and be wary of the information it requests. For example, ask yourself why a particular application or program would need access to your pictures, contact list, or other files.

RESOURCES AVAILABLE TO YOU

OnGuardOnline.gov

Learn the experts' tips for protecting your information and your computer while online, including mobile app basics and securing your wireless network.

StaySafeOnline.org

Read tips and advice for college students on how to keep your devices and information safe.

IDtheftcenter.org

Access dedicated identity theft resources along with victim and consumer support help.

IF YOU'VE BEEN COMPROMISED

- Immediately change all passwords; financial passwords first. Do not use that password in the future.
- Disconnect your computer from the Internet.
- Restart your computer in safe mode and back up your data.
- Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center at www.ic3.gov.
- Report the attack to your university and the local authorities.
- File a report with the U.S. Computer Emergency Readiness Team at www.us-cert.gov and the Federal Trade Commission at www.ftccomplaintassistant.gov.
- If you or someone you know is being stalked, call [The Stalking Resource Center National Center for Victims of Crime Helpline](http://www.the-stalking-resource-center.org).

www.dhs.gov/stopthinkconnect.

www.dhs.gov/stopthinkconnect