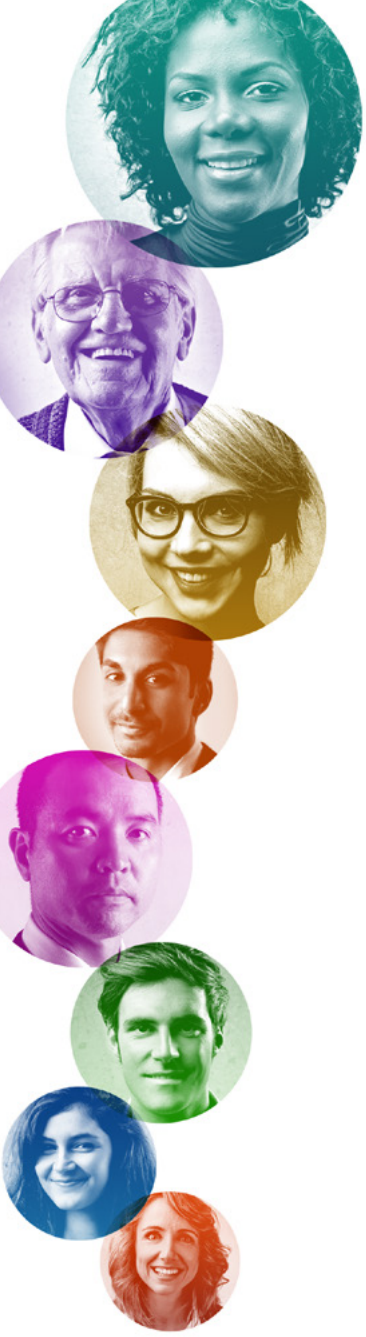


GRADES 9-12 STUDENT TIP CARD

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.

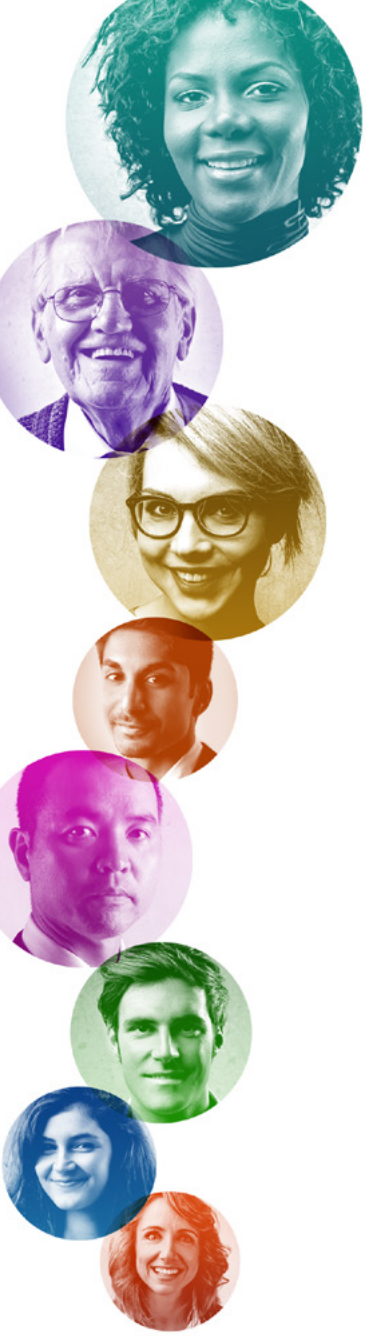
DID YOU KNOW?

- **43 percent** of teens have been victims of cyberbullying.[1]

SIMPLE TIPS

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Think before you click — don't open e-mails from strangers and don't click on links for unfamiliar sites.
8. 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.
9. Use privacy settings on social networking websites such as Twitter, Instagram, SnapChat, and Facebook.

[1] National Crime Prevention Council, http://www.ncpc.org/resources/files/pdf/bullying



10. Be cautious when downloading applications on your smartphone — they may contain malware that could infect your device.
11. 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/teach-online-safety/csave.

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.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stopthinkconnect.