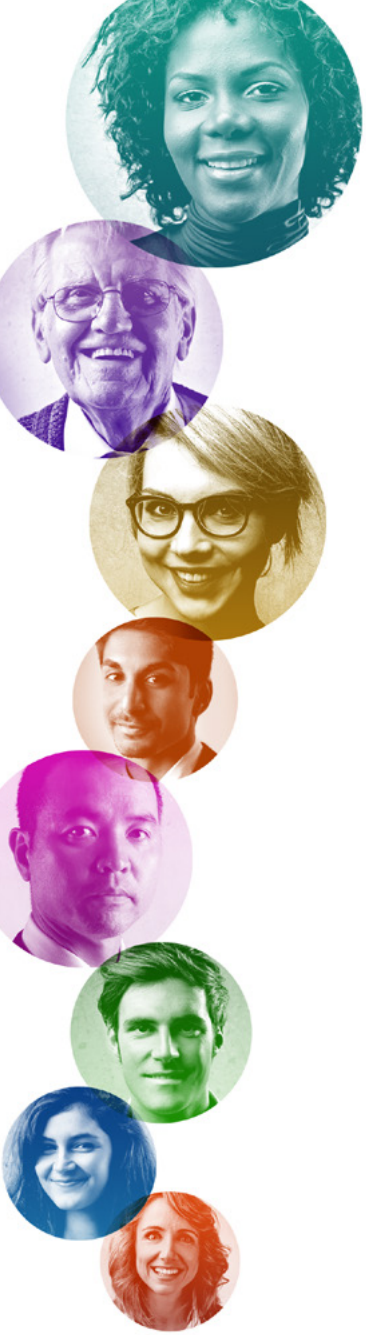


UNDERGRADUATE STUDENT TIP CARD

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.

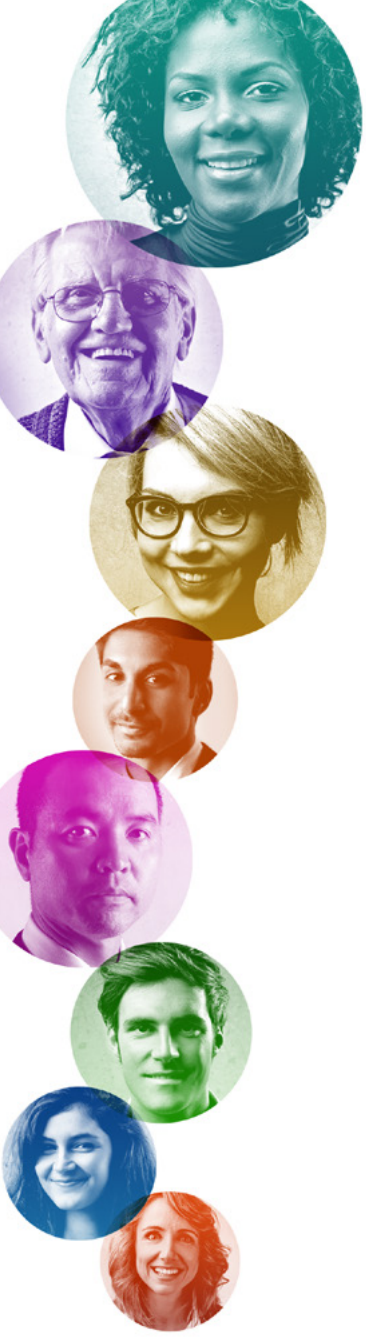
DID YOU KNOW?

- In 2012, **31 percent** of all identity theft complaints received by the Federal Trade Commission were filed by young adults.[1]

SIMPLE TIPS

1. 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.
2. 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.
3. 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.
4. When banking and shopping online, make sure the site is security enabled with "https://" or "shttp://".
5. 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.
6. If you see something inappropriate online, let the website know so they can take action.
7. Use strong passwords with eight characters or more that use a combination of numbers, letters, and symbols. Don't share your passwords with anyone.
8. 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.
9. Be cautious when downloading applications on your smartphone — they may contain malware that could infect your device.
10. 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.

[1] http://cencal.bbb.org/article/attention-college-students-43437, 2013



11. 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 picture•s, 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.ftc.gov/complaint.
- If you or someone you know is being stalked, contact The Stalking Resource Center National Center for Victims of Crime Helpline at www.victimsofcrime.org/our-programs/stalking-resource-center.

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.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™