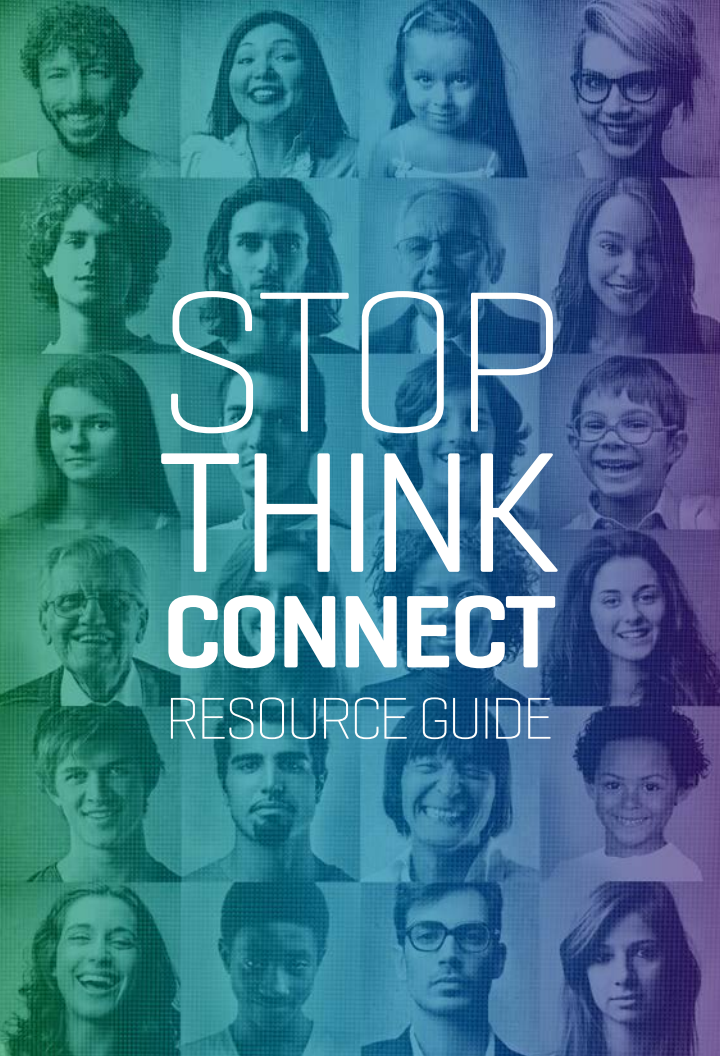


STOP THINK CONNECT

RESOURCE GUIDE

CYBERSECURITY IS A CRITICAL MISSION FOR THE DEPARTMENT OF HOMELAND SECURITY.

The U.S. Department of Homeland Security (DHS) is responsible for safeguarding the Nation from physical and cyber threats that can affect national security, public safety, and economic prosperity.

The Department's Stop.Think.Connect.™ Campaign engages with partners at all levels including government, academia, industry, and an extensive non-profit network in an effort to empower the American public to be safer and more secure online.

CYBERSECURITY IS STRONGER WHEN WE ALL DO OUR PART.

The Stop.Think.Connect. Resource Guide provides all of the tools to host a classroom discussion, a community meeting, or a workplace event about online safety. Included in the guide are:

» Easy-to-follow presentations for a wide range of audiences.

» Handouts, activities, discussion questions, and more.

» Links to supplementary information and materials to help tailor your conversation to the group you are hosting.

AUDIENCES

COLLEGE STUDENTS	INDUSTRY PROFESSIONALS
PARENTS & EDUCATORS	GOVERNMENT
YOUNG PROFESSIONALS	LAW ENFORCEMENT
SMALL BUSINESS	OLDER AMERICANS

Get resources and tips for each audience at **www.dhs.gov/stopthinkconnect**

CYBERSECURITY STARTS WITH YOU.

Whether you are an employer, a teacher, a government worker, or even a student, you have an impact on cybersecurity. By practicing strong and safe online habits, you can better protect your identity and the networks you use at home, at work, and anywhere you log on.

STOP

» Others from accessing your accounts - set secure passwords.

» Sharing too much personal information.

THINK

» Before your click. Is this a trusted source?

» About what you're doing. Would you do it or share it offline?

CONNECT

» Over secure networks. Wi-Fi hotspots may not offer the same protections.

» Wisely. Trust your gut. If it doesn't seem right, then log off or delete the email.

COLLEGE STUDENTS

QUICK FACTS

31%

of all identity theft complaints **are filed by young adults**

1 in 5 teenage Internet users have received an **unwanted sexual solicitation** online

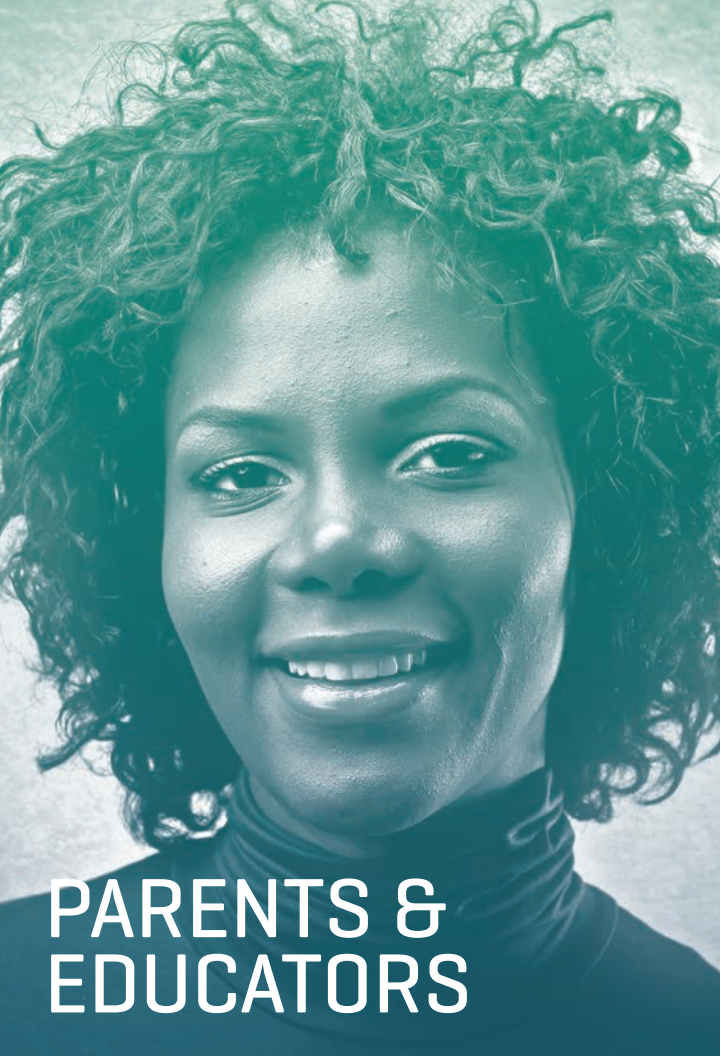
32%

of young adults say that the information about them online is **what they choose** for the public to see

SIMPLE TIPS

1. **Protect** all devices that connect to the Internet, including computers, smart phones, gaming systems, and other web-enabled devices.
2. **Keep** social security numbers, account numbers, passwords, and other personal information private.
3. **Own** your online presence. Set secure privacy settings on social networking websites and think twice about what you are posting and saying online.
4. **Check** to be sure the site is security enabled with "https://" or "shttp://" when banking or shopping online.

ⓘ **Learn** how to become a cybersecurity awareness advocate on campus: **www.dhs.gov/stopthinkconnect**.



PARENTS & EDUCATORS

QUICK FACTS

41%

of parents of teens say they monitor technology usage very closely

30%

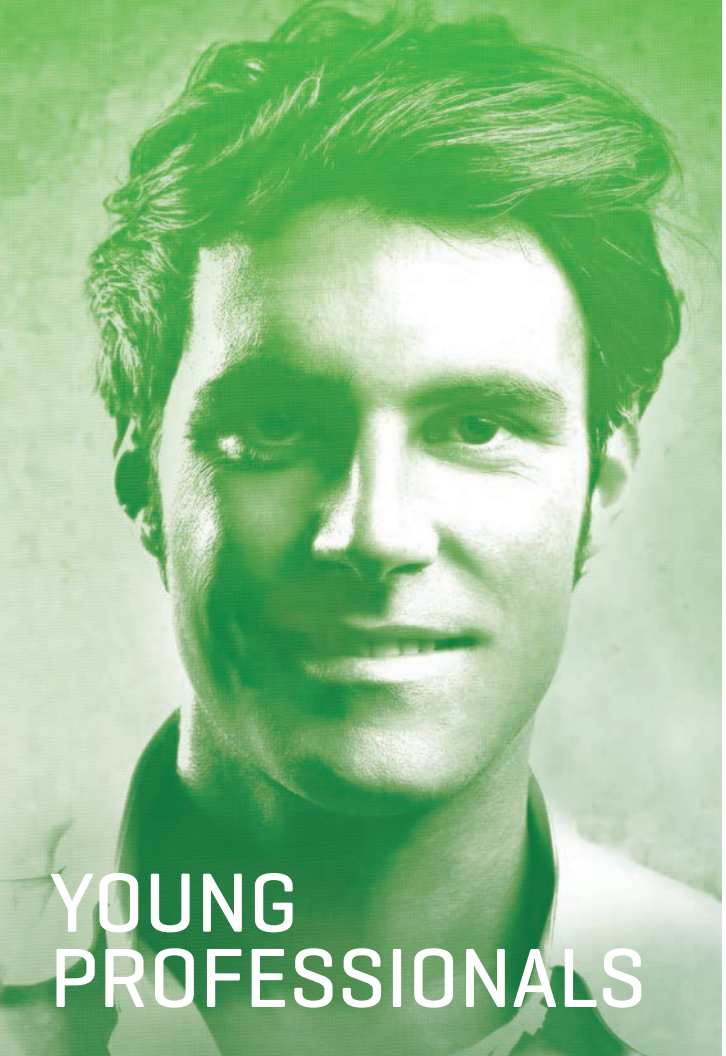
of teens have admitted to meeting someone online who claimed to be someone they were not

Seven in ten young people are victims of cyberbullying and 37% experience cyberbullying on a frequent basis

SIMPLE TIPS

1. **Create** an open and honest environment with kids.
2. **Start** conversations regularly about practicing online safety.
3. **Emphasize** the concept of credibility to teens. Not everything they see on the Internet is true.
4. **Watch** for changes in behavior. If your child suddenly avoids the computer, it may be a sign they are being bullied online.
5. **Review** security settings and privacy policies for the websites kids frequent.

ⓘ **Find** more materials for you and your children/students at **www.dhs.gov/stopthinkconnect**.



YOUNG PROFESSIONALS

QUICK FACTS

40%

of companies have a **social media policy** in the workplace

18%

of young adults claim they are **comfortable with what their friends post about them online**

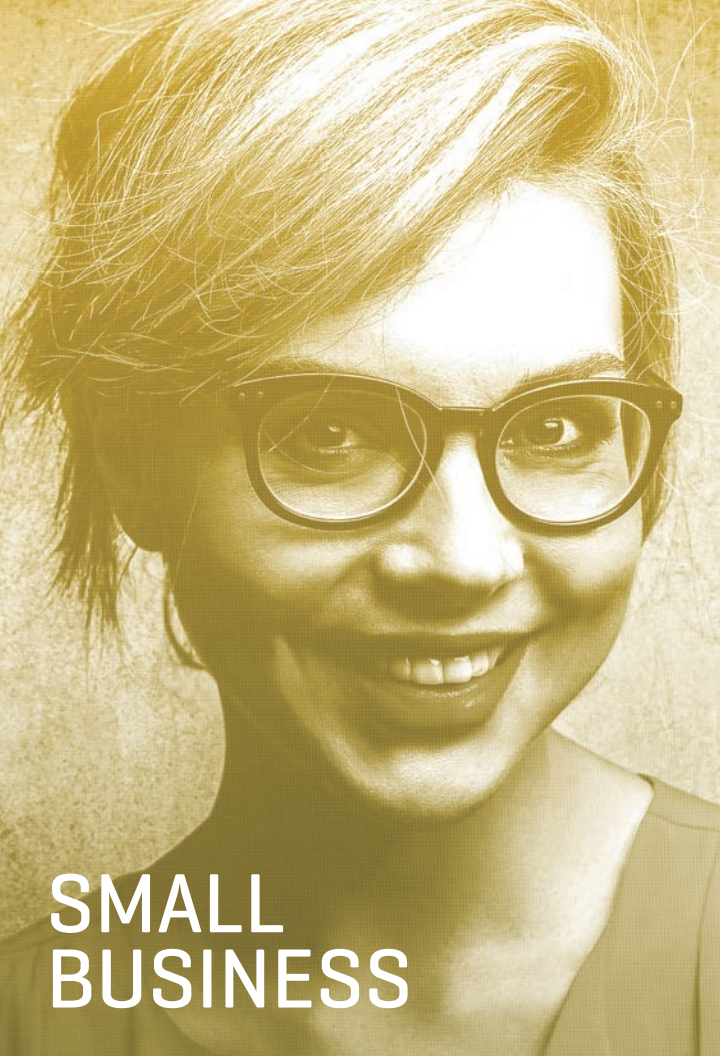
31%

of all identity theft complaints **are filed by young adults**

SIMPLE TIPS

1. **Protect** all devices that connect to the Internet, including computers, smart phones, gaming systems, and other web-enabled devices.
2. **Own** your online presence. Set secure privacy settings on social networking websites and think twice about what you are posting and saying online.
3. **Read** and follow your company's IT or Internet usage policies. Do not visit or inappropriate websites when at work or when using company devices.
4. **Think** before you act. Be wary of messages that ask for personal information.

ⓘ **Find** more tailored tips and materials at **www.stcguide.com/explore/young-professionals**.



SMALL BUSINESS

QUICK FACTS

77% of small firms believe their company is **safe from a cyber attack**

44% of small businesses reported being the **victim of a cyber attack**

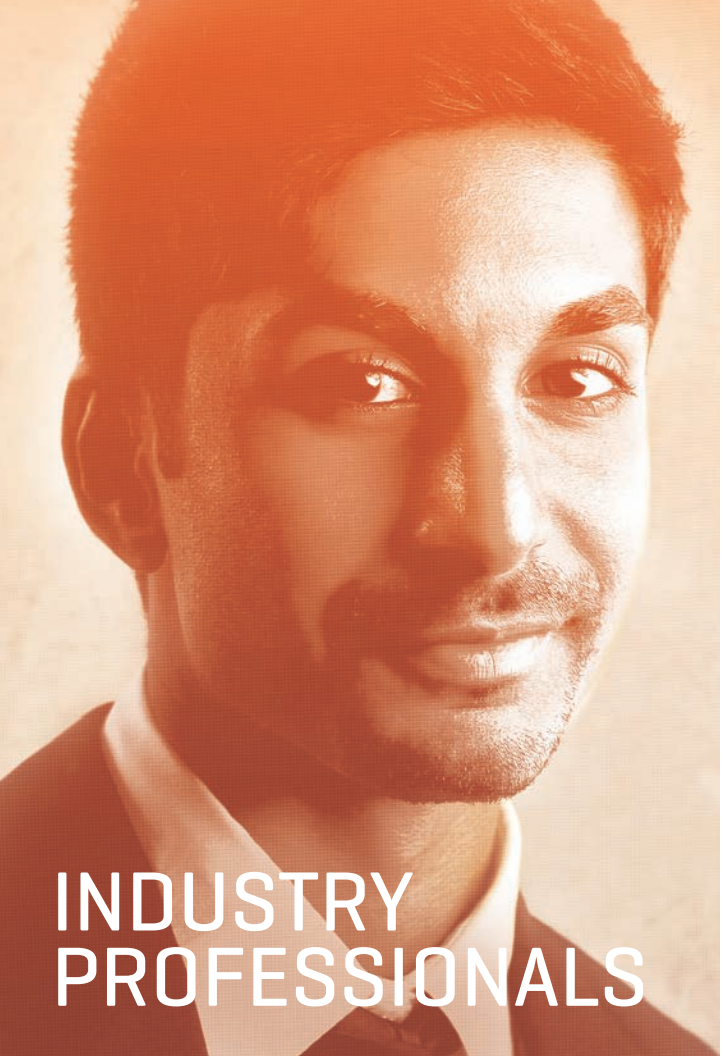
59% of small and medium sized businesses **don't have a cybersecurity contingency plan**

$9,000 — **average cost of a cyber attack**

SIMPLE TIPS

1. **Use** and regularly update antivirus and antispyware software on all computers.
2. **Secure** your Internet connection by using a firewall, encrypting information, and hiding your Wi-Fi network.
3. **Establish** security practices and policies to protect sensitive information and require employees to use strong passwords.
4. **Educate** employees and hold them accountable to Internet security guidelines and procedures.

ⓘ **Find** more resources and tools to help address cybersecurity risks at **www.us-cert.gov/ccubedvp/getting-started-smb**.



INDUSTRY PROFESSIONALS

QUICK FACTS

92% of human resources professionals said increased **vulnerability of business technology** will affect the U.S. workplace in the next 5 years

Between 2012 and 2013, the cost of cyber crime **increased $2.6 billion**.

SIMPLE TIPS

1. **Read** and abide by your company's Internet use policy.
2. **Make** your passwords complex and change them regularly (every 45 to 90 days).
3. **Keep** your user names, passwords, or other computer/website access codes private.
4. **Make** electronic and physical back-ups or copies of all your most important work.
5. **Report** all suspicious or unusual problems with your computer to your IT department.

Visit www.us-cert.gov for more industry resources.

QUICK FACTS

Federal, state, and local government agencies reported over **600,000 incidents** to the United States Computer Emergency Readiness Team (US-CERT) in fiscal year 2014.

608 million — **total number of records with sensitive information lost in data breaches since 2005**

SIMPLE TIPS

1. **Lock** and password protect all personal and company-owned devices including smart phones, laptops, notebooks, and tablets.
2. **Scan** your computer for spyware regularly and keep your software up to date.
3. **Dispose** of sensitive information properly.
4. **Protect** personal information or information about your organization, including its structure or networks. Do not provide the information unless you are certain of a person's authority to have it.

Visit www.us-cert.gov for state, local, and federal government cybersecurity alerts and resources.

LAW ENFORCEMENT

QUICK FACTS

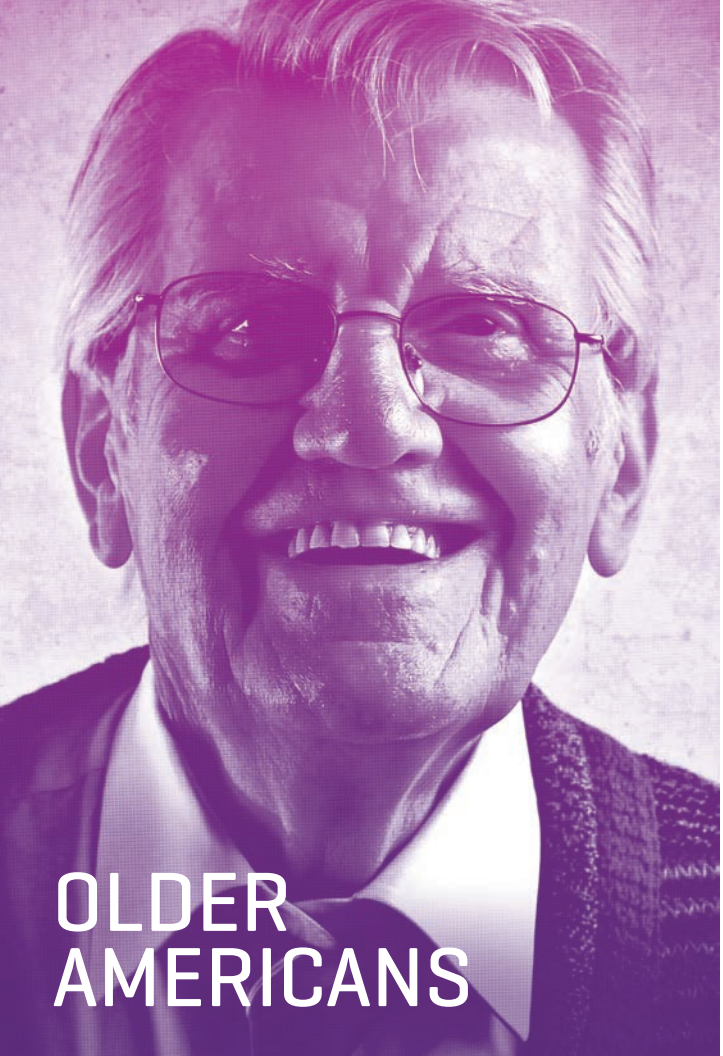
18% of local police agencies have been **victims of cyber attacks**

The FBI's Internet Crime Complaint Center receives **300,000 complaints** a year, totaling over **$800 million in losses**.

SIMPLE TIPS

1. **Shred** important documents that contain sensitive information.
2. **Know** and follow online guidelines based on your agency.
3. **Protect** sensitive information using effective passwords on computers, tablets, smart phones, and other web-enabled devices.
4. **Report** suspicious or unusual activity on your computer or web-enabled device.
5. **Beware** of the information you share in public and online.

Visit www.dhs.gov/law-enforcement for additional law enforcement resources.



OLDER AMERICANS

QUICK FACTS

Seniors are defrauded at **2x** the rate of the rest of the population.

27% **of older adults** use social networking websites

60% **of older adults** are Internet users

SIMPLE TIPS

1. **Treat** your mobile device like your home or work computer. Use strong PINS and passwords and keep software up-to-date.
2. **Use** caution when downloading or clicking on any unknown links.
3. **Create** strong passwords, combining upper and lowercase letters with numbers and special characters. Don't share passwords with anyone.
4. **Beware** of what you receive or read online. If it sounds too good to be true, it probably is.
5. **Avoid** adding people you don't know on social media websites and programs or mobile applications.

ⓘ **Find** more materials to read and share at **www.dhs.gov/stopthinkconnect**.

CONNECT WITH US

Get involved with the Stop.Think.Connect. Campaign

www.dhs.gov/stopthinkconnect

stopthinkconnect@dhs.gov

@dhsgov

@cyber | @uscert_gov | @STOPTHNKCONNECT

www.facebook.com/homelandsecurity
www.facebook.com/STOPTHINKCONNECT

www.youtube.com/user/StaySafeOnline1

GET RESOURCES AND TIPS TO HELP YOU STAY SAFE ONLINE

www.dhs.gov/stopthinkconnect

Homeland Security

STOP | THINK | CONNECT

Stop.Think.Connect.™ is a national public awareness campaign conducted by the Department of Homeland Security in cooperation with the National Cyber Security Alliance. For more information, contact us at stopthinkconnect@dhs.gov.