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

» An easy-to-follow presentation with supporting PowerPoint slides and draft script.

» Handouts, activities, discussion questions, and more.

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

Get resources and tips for any 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. Wifi hotspots may not offer the same protections.

» Wisely. Trust your gut. If it doesn’t seem right, then close out or delete the email.
Protect all devices that connect to the Internet, including computers, smart phones, gaming systems and other web-enabled devices.

Keep social security numbers, account numbers, passwords, and other personal information private.

Own your online presence. Set secure privacy settings on social networking websites and think twice about what you are posting and saying online.

Check to be sure the site is security enabled with “https://” or “shttp://” when banking or shopping online.

Think before you act. Be wary of messages that ask for personal information.

QUICK FACTS

- 31% of all identity theft complaints made to the FTC are made by young adults.
- 37% of employers use social networking to research job candidates.
- 1 in 5 teenage Internet users have received an unwanted sexual solicitation online.

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.
5. Think before you act. Be wary of messages that ask for personal information.
PARENTS & EDUCATORS
Create an open and honest environment with kids.

Start conversations regularly about practicing online safety.

Emphasize the concept of credibility to teens. Not everything they see on the Internet is true.

Watch for changes in behavior. If your child suddenly avoids the computer, it may be a sign they are being bullied online.

Review security settings and privacy policies for the websites kids frequent.
YOUNG PROFESSIONALS
Protect all devices that connect to the Internet, including computers, smart phones, gaming systems and other web-enabled devices.

Own your online presence. Set secure privacy settings on social networking websites and think twice about what you are posting and saying online.

Check to be sure the site is security enabled with “https://” or “shttp://” when banking or shopping online.

Think before you act. Be wary of messages that ask for personal information.

Encourage your colleagues, families, and communities to be web wise.

QUICK FACTS

- 21% of all identity theft victims in 2012 were ages 20-29
- 61% of employers currently use, or plan to use, social media in their recruiting efforts
- 33% of companies have a social media policy in the workplace

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. Check to be sure the site is security enabled with “https://” or “shttp://” when banking or shopping online.
4. Think before you act. Be wary of messages that ask for personal information.
5. Encourage your colleagues, families, and communities to be web wise.
SMALL BUSINESS
Use and regularly update antivirus and antispyware software on all computers.

Secure your Internet connection by using a firewall, encrypting information, and hiding your Wi-Fi network.

Establish security practices and policies to protect sensitive information.

Educate employees and hold them accountable to Internet security guidelines and procedures.

Require that employees use strong passwords and regularly change them.

**QUICK FACTS**

- **31%** of all cyber attacks targeted businesses with fewer than 250 employees.
- **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.

4. Educate employees and hold them accountable to Internet security guidelines and procedures.

5. Require that employees use strong passwords and regularly change them.
Read and abide by your company’s Internet use policy.

Make your passwords complex and change them regularly (every 45 to 90 days).

Keep your user names, passwords, or other computer/website access codes private.

Make electronic and physical back-ups or copies of all your most important work.

Report all suspicious or unusual problems with your computer to your IT department.

QUICK FACTS

- 92% of human resources professionals said increased vulnerability of business technology will affect the U.S. workplace in the next 5 years.
- 64% of data breaches can be accounted for by employee negligence and system glitches together.
- 75% of cyber attacks are opportunistic – not targeted at a specific individual or company.

SIMPLE TIPS
GOVERNMENT
Lock and password protect all personal and company-owned devices including smart phones, laptops, notebooks, and tablets.

Scan your computer for spyware regularly and keep your software up to date.

Dispose of sensitive information properly.

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.

**QUICK FACTS**

The Federal Government faces millions of cyber attacks per day.

Information security incidents at 24 federal agencies have increased 650% in the past 5 years.

48% of government data breaches stem from accidental exposure from inside the enterprise.

**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.
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.

**QUICK FACTS**

More than \( \frac{2}{3} \) of cyber incidents reported to the federal government are phishing attempts.

**Cybercrime costs** the world significantly more than the global black market in marijuana, cocaine, and heroin combined.

**SIMPLE TIPS**
Treat your mobile device like your home or work computer. Use strong PINS and passwords and keep software up-to-date.

Use caution when downloading or clicking on any unknown links.

Create strong passwords, combining upper and lowercase letters with numbers and special characters, and don’t share them with anyone.

Beware of what you receive or read online—if it sounds too good to be true, it probably is.

Avoid adding people you don’t know on social media sites and programs like Skype.

QUICK FACTS

- 69% of people over 65 have a mobile phone
- 53% of people over 65 are Internet users
- 34% of Internet users age 65 and older use social networking sites

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, and don’t share them 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 sites and programs like Skype.
GET RESOURCES AND TIPS TO HELP YOU STAY SAFE ONLINE

www.stopthinkconnect.org/resources

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.