STOP.THINK.CONNECT™

NATIONAL CYBERSECURITY AWARENESS CAMPAIGN
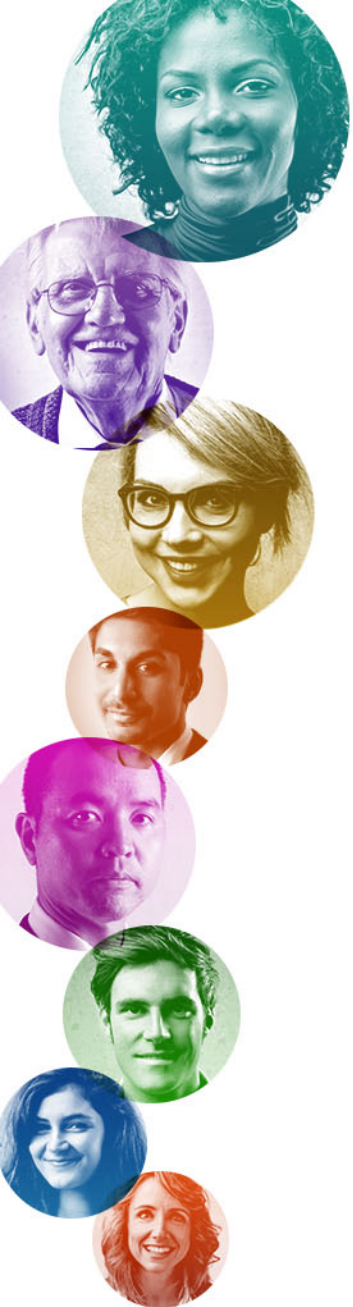# KIDS PRESENTATION

Homeland Security

STOP | THINK | CONNECT

ABOUT STOP.THINK.CONNECT.™

- In 2009, President Obama asked the Department of Homeland Security to create the Stop.Think.Connect. Campaign to help Americans understand the dangers that come with being online and the things we can do to protect ourselves from cyber threats.

- Stop.Think.Connect.™ reminds Americans that cybersecurity is a shared responsibility – at home, at school, and in our communities.

STOP | THINK | CONNECT

Homeland Security

WHAT IS CYBERSPACE?

Cyberspace is anything that has to do with the Internet.

- We use the Internet to communicate and stay connected to our friends and family.

- We play video games, download music, and watch TV shows and movies **after** homework is done.

- Grownups do things like banking, shopping, and other important everyday activities online too.

WHY DO WE NEED TO PROTECT CYBERSPACE?

- Crimes that happen in real life – such as stealing – also happen on the Internet.

- Just like you have to look both ways before crossing the street, you have to be careful when using the Internet.

- The Department of Homeland Security helps you protect yourself from dangers on the Internet by teaching you what to look out for online.

- Often, we might not realize that our actions online might hurt us, our families, and even our country. Learning about the dangers online and taking action to protect ourselves is the first step in making the Internet a safer place.

KIDS LEAD DIGITAL LIVES

- Kids ages 8-18 spend *7 hours and 38 minutes* per day online

- If a child sleeps 8 hours per night, that means **ONE HALF** of the time that he or she is awake is spent online
  - 33% Online
  - 33% Offline (awake)
  - 33% Asleep

- Some common online issues kids face include:
  - Cyber Predators
  - Cyber Bullying
  - Identity Theft

Source: National Cyber Security Alliance

STOP | THINK | CONNECT

Homeland Security

CYBER PREDATORS & BULLIES

Cyber predators *are people who search online for other people in order to use, control, or harm them in some way.*

Cyberbullying *is the electronic posting of mean-spirited messages about a person, often anonymously.*

Cyber Tips for Kids

- Keep your personal information private; avoid sharing your name, address, telephone number, birthday, passwords, and the name of your school when using the Internet.

- Think twice before you post or say anything online; once it is in cyberspace, it's out there forever.

- Treat others like you want to be treated.

- 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.

STOP | THINK | CONNECT

Homeland Security

IDENTITY THEFT

Identity theft *is the illegal use of someone else's personal information to steal money or credit.*

Cyber Tips for Kids

- If you have your own email account, let your parents know if you ever receive an email that asks for your personal information. Some emails look official, as if they were sent from a club or school, but they could be a trick to get your personal information. Fake emails usually seem urgent, and ask you to respond with your private information.

- Choose a screen name or email address that isn't your real name to protect your identity. For instance, instead of "Jack Smith," why not choose "Sk8boardKing75?"

- Create strong passwords with eight characters or more that use a combination of letters, numbers, and symbols. Don't share your passwords with anyone.

- Think before you click – don't open emails from strangers and don't click on links for unfamiliar sites.

- Use and check your privacy settings on social networking sites like Facebook and Twitter.
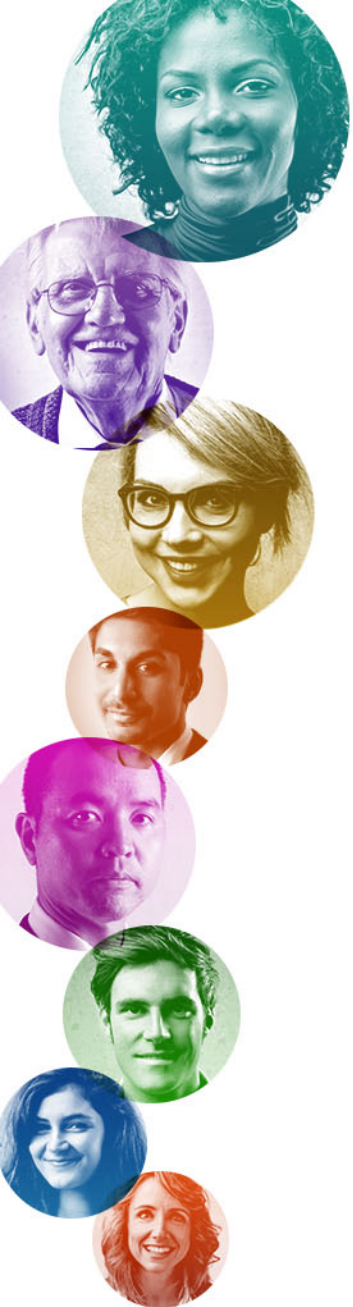
Homeland Security

MOBILE SECURITY

When you play games, video chat, or surf the web on a cell phone or tablet, you are accessing the Internet on the go. We need to be careful when using cell phones just like we are careful when using a computer.

Cyber Tips for Kids

- **Keep a close eye on your mobile device.** Never leave your mobile devices unattended.

- **Keep It Locked.** Always lock your device when you are not using it. Use strong passwords to prevent others from accessing your device. Never share your passwords with someone other than your parent or guardian.

- **Know Your Apps**. Check with your parents before you download an app and review the settings with them.

- **Only Connect to the Internet if Needed.** Disconnect your device from the Internet when you aren't using it and make sure your device isn't set to automatically connect to Wi-Fi.

COMMON SENSE RULES APPLY ONLINE

- **Don't talk to strangers**. Don't communicate with strangers online and never agree to meet in person. Tell a parent, teacher, or an adult you trust if a stranger contacts you in a chat room, through email, or via text messaging.

- **Look both ways before crossing the street**. Don't enter contests, join clubs, or share your personal information for any reason, unless your parents say it's OK. Your name, address, age, phone number, birthday, email address, where you go to school, and other facts about you are personal and shouldn't be shared without checking first.

- **If the offer seems too good to be true, then it probably is**. How many of you have ever received an email offering something free, like a cell phone or concert tickets? These are tricks designed to get you to give up personal information or click on links to automatically install malware or spyware.

STOP | THINK | CONNECT

Homeland Security

WE NEED YOUR HELP!

- The Department of Homeland Security can't protect the Internet alone. We need help from all Americans – including everyone here – to make smart and safe decisions when using the Internet.

- Once we understand the dangers, we need to tell other people who might not be as cyber smart and savvy. Setting a good example of online behavior is something you can do right now to make a difference.

- That's why cybersecurity begins with you. Yes, **you**! Every Internet user, no matter how young or old, is our Nation's first line of defense against people who might want to harm us.

- If we all become more aware of who we talk to, what we say, and what we share online – we can make a big difference.

STOP | THINK | CONNECT

Homeland Security

CYBER EDUCATION

The Stop.Think.Connect. Campaign also promotes science, technology, engineering, and math (STEM) education among students.

- To help keep our computers and our country's networks safe, we need more cybersecurity professionals.

- To do that, we need students who have skills in **science, technology, engineering, and math.**

- To learn more about STEM education and careers, visit the National Initiative for Cyber Careers and Studies (NICCS) Portal at www.niccs.us-cert.gov/.

SCENARIO #1:
AIMEE'S COUNTRY COUNTDOWN

Aimee loves listening to country music any chance she gets and regularly downloads her favorite songs onto the new MP3 Player her parents bought for her birthday. They gave her firm guidelines for downloading music—one of the rules is that she must ask them to approve the website she gets the music from to be sure it is a legitimate website and is legally downloaded. Lately she has been downloading a lot of great tunes, so her parents finally said, "No more! You have enough songs!"

Aimee's friend at school just told her about the best country song from a new country band's album. Aimee loves this band and just has to have the new album! Her friend tells her about a secret website where you can download this new album and get all the songs for free. Aimee questions this for a minute, but trusts her friend, and eventually decides to download the new album as soon as she gets home from school. She finds the website and begins answering the questions the website requires. These include name, address, birthday, and email address. At the bottom of the webpage, the website has an additional link that offers 10 hit songs a month for only $1.99, but requires a credit card number to activate.

- What should Aimee do?

- What were Aimee's mistakes?

- Did Aimee do anything illegal?

- Is Aimee's friend truly a friend?

- Who were Aimee's actions most unfair to? Why?

SCENARIO #2:
JAKE AND THE BAD VIRUS

Jake was using the Internet on his family's home computer to research a school project on dolphins. He just finished finding the perfect article to add to his research and was about to log off the computer. Before shutting down Jake decides to quickly check his email account. In his inbox, Jake sees two messages including one from NO1GRANDPA@HAPPYMAIL.COM, which he recognizes as his Grandfather's email address, and another from SWEEPSTAKES@WHOKNOWS.COM with a subject line that reads —YOU'VE WON $5,000.

Jake skips his Grandfather's email and quickly opens the sweepstakes email to collect his prize. After doing so, Jake receives a message instructing him to provide personal information to verify his identity. Jake provides his full name, birthday, home address and phone number. He hits submit and instantly starts receiving messages saying his computer has been infected by a virus. Jake panics because he doesn't want to get into trouble. He quickly logs off, shuts off his computer, and goes to bed, hoping his parents won't know what happened in the morning.

- What were Jake's mistakes?
- What should Jake have done?

STOP | THINK | CONNECT

Homeland Security