HEADS UP

STOP THINK CONNECT

OnGuard Online

STOP | THINK | CONNECT™

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.

OnGuardOnline.gov provides practical tips from the federal government and the technology community to help you guard against Internet fraud, secure your computers, and protect your privacy.

Please visit **www.dhs.gov/stopthinkconnect** for more information on Stop.Think.Connect. programs and opportunities.

TABLE OF CONTENTS

STOP
THINK
CONNECT
APPS
PRIVACY
RESPECT
DOWNLOAD
TEXTING
POLITENESS
PROFILE
VIRTUAL
SECURITY
SPYWARE

WORD SEARCH

T	T	L	N	A	S	T	O	P	E	E
T	L	R	S	I	E	I	D	G	A	R
P	R	I	V	A	C	Y	P	N	T	A
D	I	P	L	A	U	T	R	I	V	W
S	A	G	Y	O	R	R	S	T	R	Y
A	G	O	F	A	I	N	X	X	E	P
K	P	O	L	I	T	E	N	E	S	S
N	R	P	P	N	Y	Y	W	T	P	V
I	P	V	S	W	W	S	P	P	E	T
H	R	E	L	I	F	O	R	P	C	T
T	C	E	N	N	O	C	D	R	T	P

You text, you play games, you share photos and video. You update your status, you post comments, you probably spend some time in a virtual world.

Being online—connected through some sort of device—is how you live your life. And as you spend more of your time there, it can be easy to over-share, embarrass yourself, mess up your computer, and possibly get messages from creepy people. The truth is there are some risks involved in socializing, playing, and communicating online.

Regardless of how fast your fingers fly on a keyboard or cell phone, the best tool you have to help avoid risks online is your brain. When you're ready to post or send a message or a photo, download a file, game or program, or shop for something—stop for a second. Think about things like:

Do you know and trust who you're dealing with—or what you're sharing or downloading?

How will you feel if your information ends up somewhere you didn't intend?

Asking a few key questions first can help you protect yourself, your friends and your computer. Flip through and find more things to stop and think about before you connect.

SHARE WITH CA

Your online actions can have real-world consequences. The pictures you post and the words you write can affect the people in your life. Think before you post and share.

What you post could have a bigger "audience" than you think. Even if you use privacy settings, it's impossible to completely control who sees your social networking profile, pictures, videos, or texts. Before you click "send," think about how you will feel if your family, teachers, coaches, or neighbors find it.

Once you post information online, you can't take it back. You may think that you've deleted information from a site—or that you will delete it later. Know that older versions may exist on other people's computers. That means your posts could live somewhere permanently.

Get someone's okay before you share photos or videos they're in. Online photo albums are great for storing and sharing pictures of special events, and camera phones make it easy to capture every moment. Stop and think about your own privacy—and other people's—before you share photos and videos online. It can be embarrassing, unfair, and even unsafe to send or post photos and videos without getting permission from the people in them.

PROTECT YOUR COMPUTER

Be cautious about opening attachments or clicking on links. They may contain viruses or spyware.

Learn about security software and how your home computer, the kids' laptop, and their computer tablets are protected. Maintain up-to-date antivirus software on all your devices that connect to the Internet to increase your devices' security.

Remember that, sometimes, free stuff—like games, ring tones, or screen savers—can hide viruses or spyware. Don't download unless you trust the source and scan the file with security software.

Use peer-to-peer (P2P) file-sharing services with caution. Make sure you install file-sharing software properly, and scan downloaded files with security software before you open or play them. Otherwise, you could be sharing information your family expects to keep private, like financial records.

PROTECT YOUR INFORMATION

Some information should stay private.

Your Social Security Number and family financial information—like your parents' bank account or credit card numbers—should stay in the family.

Keep passwords private. The longer and more complex your password, the harder it is to crack. Don't share your passwords with anybody, including your best friends or your boyfriend or girlfriend.

Don't reply to text, email or pop-up messages that ask you to reply with personal information–

even if the message looks like it comes from a person, company or organization you know, or threatens that something bad will happen if you don't reply. These messages may be fakes, sent to steal your information.

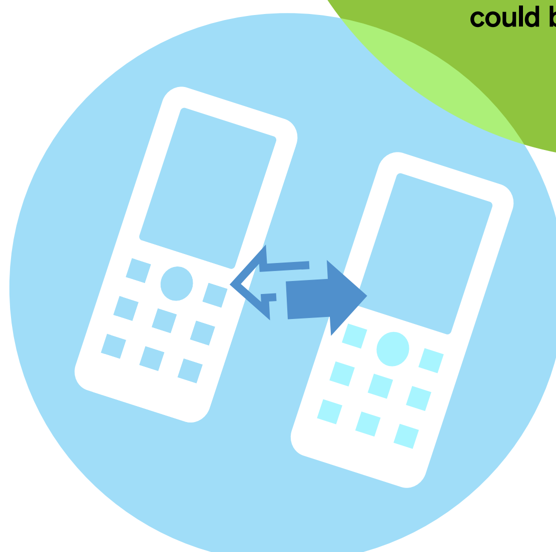
Have you ever downloaded something that turned out to be different than you expected?

RE

Were you ever sorry you shared something online?

SEXTING

You may have heard stories at school or in the news about people "sexting"—sending nude photos from mobile phones. Don't do it. Period. People who create, forward or even save sexually explicit photos, videos or messages put their friendships and reputations at risk. Worse yet, they could be breaking the law.



INTERACT WITH CONNECTION

Politeness counts. Texting is just another way for people to have a conversation, and texters are just like people talking face-to-face or on the phone: they appreciate “please” and “thank you” (or *pls* and *ty*).

Tone it down. In online conversations, using ALL CAPS, long rows of exclamation points, or large, bolded fonts is the same as shouting.

Use “Cc:” and “Reply All:” sparingly. Before you hit send on an email, stop and think about whether everyone needs to see that message.

Avatars are people too. When you’re playing a game or exploring an online world where you can create a character and interact with others, remember real people are behind those characters on the screen. Respect their feelings just

THE PROTECTION TACT

PROTECT YOURSELF

Use privacy settings to restrict who can see and post on your profile. Many social networking sites, chat rooms, and blogs have privacy settings. Find out how to turn these settings on, and then do it.

Limit your online friends to people you actually know. The people you meet on the Internet may not be who they appear to be.

Learn about social mapping. Many mobile phones have GPS technology, and there are applications that allow you to find your friends—and allow them to find you. Use GPS and social mapping apps only with people you know personally and trust. Take advantage of privacy features in apps and on your phone.

Trust your gut if you feel threatened or uncomfortable because of someone or something you find online. Tell someone who can help you report your concerns to the proper authorities and other people who can help.

Have you seen something online that made you angry?

like you would in person. Remember that your character or avatar is a virtual version of you—what does it tell people about you and your interests?

Don't impersonate. It's wrong and can be hurtful to create sites, pages, or posts that seem to come from someone else, like someone in your class or a teacher.

Speak up. If you see something inappropriate on a social networking site or in a game or chat room, let the website know and tell an adult you trust. Using "Report Abuse" links can help keep sites fun for everyone.

Don't stand for bullying—online or off. Treat others the way you want to be treated—whether you're interacting with them online, on your phone or in person.

CYBERBULLYING

Cyberbullying is bullying that happens online. It can happen in an email, a text message, an online game, or on a social networking site. It might involve rumors or images posted on someone's profile or passed around for other people to see.

You know that, right? So you know that cyberbullying is a lose-lose proposition: it often makes the person being harassed feel bad—and it makes the bully look bad. It also might lead to punishment from school authorities or the police.

What do you do if you witness cyberbullying?

Tell the bully to stop. Most kids don't bully, and there's no reason for anyone to put up with it. This mean behavior usually stops pretty quickly when somebody stands up for the person being bullied.

Avoid being a cyberbully and practice good cyber ethics. Follow the Golden Rule: Be nice online and in real life. Don't say or do anything online that you wouldn't do in person. Own what you say and do online.