

HEADS UP

STOP

THINK

CONNECT



STOP THINK CONNECT

**OnGuard
Online.gov**

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 is the federal government's website to help you be safe, secure and responsible online.

To order free copies of this brochure, visit bulkorder.ftc.gov.

July 2013

**OnGuard
Online.gov**

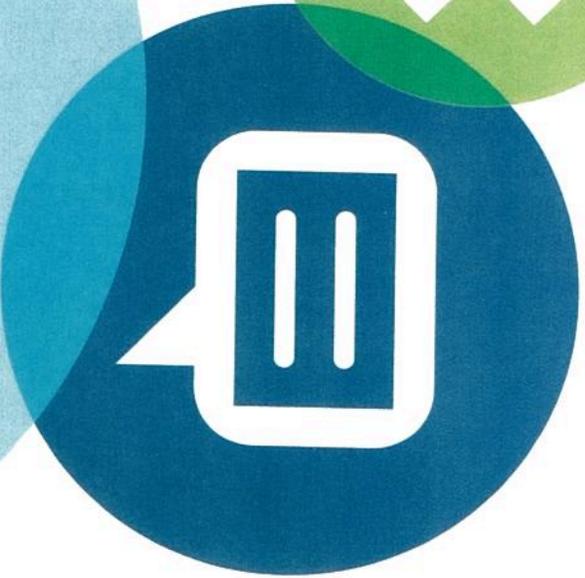


TABLE OF CONTENTS

- 2 Share with Care
- 4 Interact with Tact
- 8 The Protection Connection
- 12 Word Search

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, phone or tablet, 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 click.

SHARE WITH CARE

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.

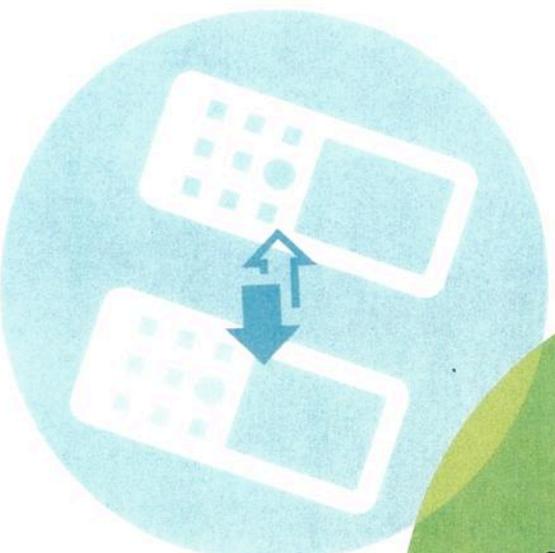
Get someone’s okay before you share photos or videos they’re in. Online photo albums are great for storing and sharing pictures. It’s so easy to snap a shot and upload it instantly. Stop and think about your own privacy—and other people’s—before you share photos and videos online. It can be embarrassing, unfair and even unsafe to send or post photos and videos without getting permission from the people in them.

Sexing: Don’t do it. You may have heard stories at school or in the news about people “sexing”—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.

Were you ever sorry you shared something online?

Once you post something online, you can’t take it back.

You may think that you’ve deleted a comment or a picture from a site—or that you will delete it later. Know that it may still be online or saved on someone else’s computer.



INTERACT WITH TAGT

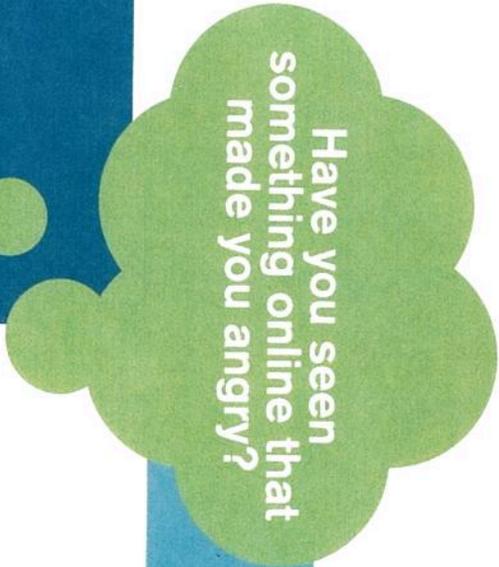


Politeness counts. Texting is just another way for people to have a conversation, and texts are just like people talking face-to-face or on the phone: they appreciate “please” and “thank you” (or *pls* and *ty*).

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 send a message, stop and think about whether everyone needs to see it.

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



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.

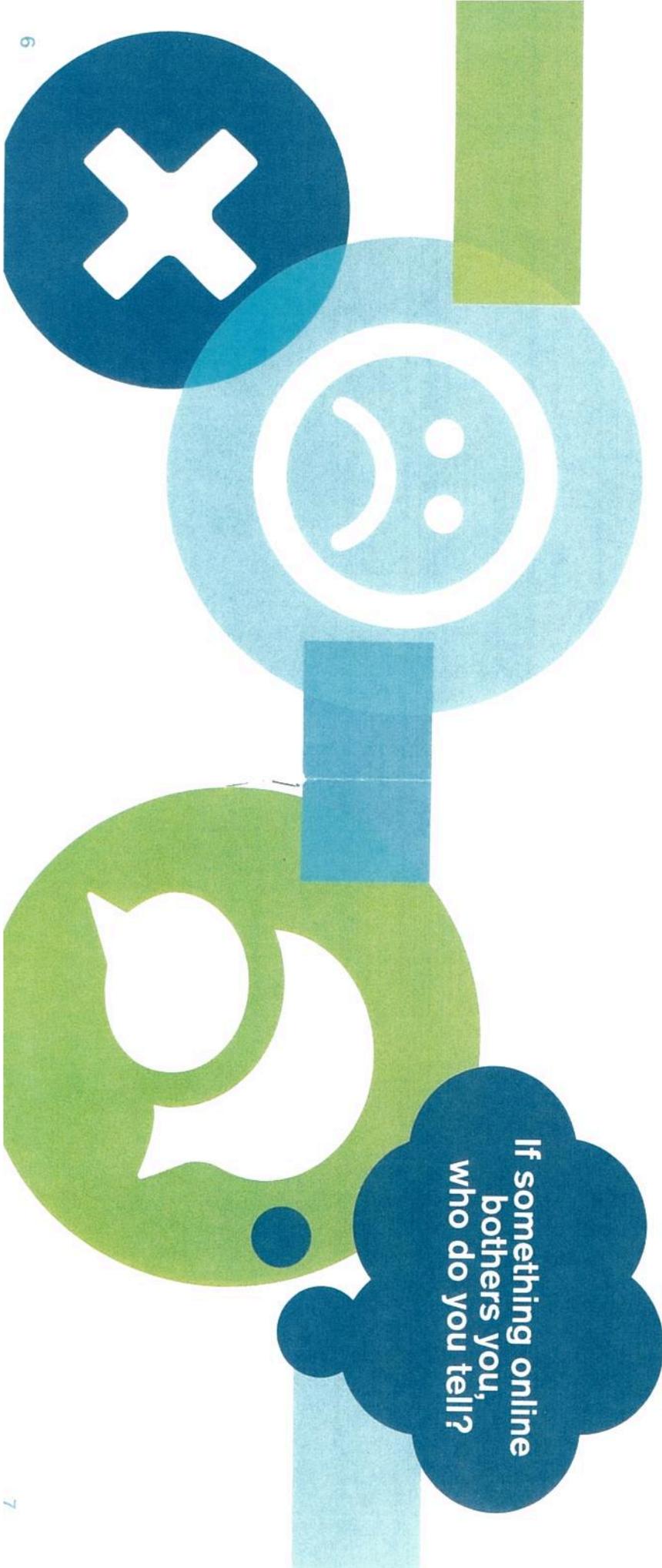
CYBERBULLYING

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 someone harasses you online? Keep a cool head, and don't respond. Most people realize that bullying is wrong. Sometimes you can stop bullying if you ignore or block the person. You also can report abuse to the website where it's taking place. If it continues, save the evidence and ask for help from an adult you trust.

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.

A stylized illustration of a person's head in profile, facing right. The head is green with a white speech bubble inside. A blue thought bubble is attached to the bottom of the head. The background consists of various colored shapes: a green rectangle at the top, a light blue circle containing a sad face, a dark blue circle containing a white 'X', and a light blue rectangle at the bottom.

If something online bothers you, who do you tell?

THE PROTECTION CONNECTION

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.

Learn about location-based services. Many phones have GPS technology, and there are applications that let you find out where your friends are—and let them find you. Set your privacy settings so that only people you know personally can see your location. Think about keeping location-based services off, and turning them on only when needed. Ask yourself, “Does this app need to know where I am?”

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 police and other people who can help.

Do you download apps? If you do, you might be giving the app's developers access to your personal information—maybe even info that's not related to the purpose of the app. For example, say you download an app that lets you make a drawing out of a photo, but the company who made the app gets access to your entire contact list. It might share the information it collected with marketers or other companies.

You can try to check what information the app collects—if it tells you—and check out your own privacy settings. Also think about whether getting that app is really worth sharing the details of your life.

Some apps cost money. And many free apps let you buy stuff within them—with real money. Check with your parents to make sure they're ok with you buying additional features, especially if they're paying the bill.

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 your passwords private. The longer 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's from a friend, family member or company 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?

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 computers are protected.

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.

Whether it's your laptop, tablet or phone, don't leave it in public—even for a minute. If it goes missing, all the important information stored on it—like your messages and photos—may fall into the wrong hands.



WORD SEARCH

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

