

HEADS UP

STOP

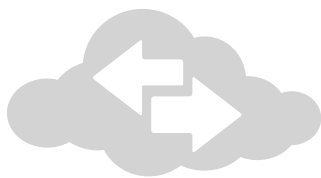
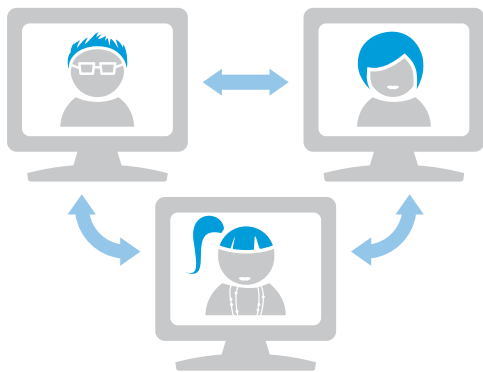
THINK
CONNECT



FTC.gov/
OnGuardOnline 

YOU PROBABLY SPEND TIME:

connecting with friends and family online



downloading apps



sharing what you're doing — and where you are



sharing photos and videos on-the-go

building your online profiles and reputation



WHY SHOULD I READ THIS?

The truth is there are some risks involved in posting, playing, and talking to people online. It can be easy to over-share, embarrass yourself, mess up your computer, and possibly get messages from creepy people.

Asking a few key questions first can help you protect yourself, your friends, your accounts, and your devices.

Before you post a message or a photo, download a game, or buy something online...

ask yourself:

How will I feel if my photos or comments end up somewhere I didn't mean for them to be?

Do I know and trust who I'm dealing with?

SHARE WITH CA

Your online actions can have real-world consequences. The photos, videos, and messages you share can affect the people in your life. Think before you post.

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 profile, pictures, videos, or texts. Think about how you will feel if your family, teachers, coaches, or neighbors find it.

Get someone’s OK before you share photos or videos they’re in. It can be embarrassing, unfair, and even unsafe to send or post photos and videos without getting permission from the people in them.

Sexting: Don’t do it.

You may have heard stories at school or in the news about people “sexting” — sending nude photos from their 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.

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

Even if you delete it, that photo or comment you don't want people to see anymore could be living somewhere — permanently.

Were you ever sorry you shared something online?



INTERACT WITH

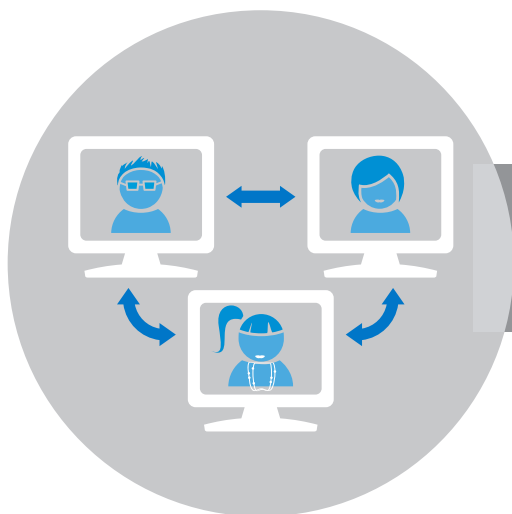


Politeness counts. Quick texts can lead to misunderstandings — so think about how your message might be read and understood before you send.

Take it easy. Using all CAPS, long rows of exclamation points, or large bolded fonts is the same as shouting. AND NO ONE LIKES TO BE YELLED AT!!!!

Send group messages with care. Think about who needs to see your message before sending to multiple people.

TACT



Remember what's real. When you're playing a multi-player game, keep in mind that real people are behind those characters on the screen. Respect their feelings just like you would in person.


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

Speak up. If you see a friend post something thoughtless, tell them. You may help your friend keep out of trouble and avoid looking foolish. If you see something inappropriate on social media or in a game, let the website know and tell an adult you trust. Using Report Abuse links can help keep sites fun for everyone.

STAND UP TO CY

Cyberbullying is bullying that happens online. It can happen in a text message, an online game, or on social media. It might involve trolling, rumors, or images posted on social media or passed around for other people to see.

Bullying often makes the person being harassed feel bad — and it makes the bully look bad. It also might get you in trouble with your school or the police.



Treat others the way you want to be treated — whether you're online or in person.



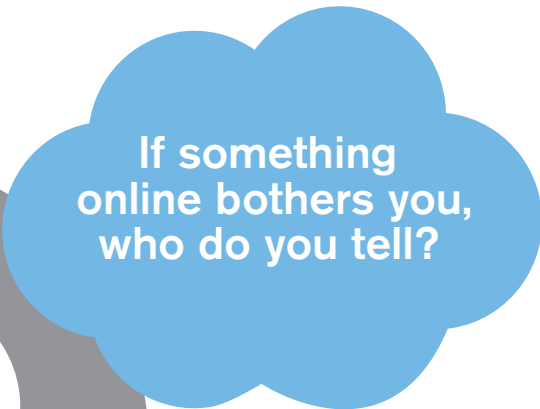

Y BERBULLYING

What if someone harasses you online?

- Keep a cool head, and don't be mean back. Most people realize that bullying is wrong.
- Ignore or block the person.
- Report abuse to the website where it's taking place.
- Save the evidence and ask for help from an adult you trust.

What 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.



If something
online bothers you,
who do you tell?

THE PROTECTION

PROTECT YOURSELF

Use privacy settings. Find out how to turn on privacy settings on your apps and social media — then do it.

Think about when it makes sense to turn off your location. There are apps that let you find out where your friends are — and let them find you. Use location features only with people you know personally. And for other apps, ask yourself, “Does this app need to know where I am?”



Limit your online friends to people you actually know.

Did you know? When you post a photo you took on your phone, it could also have information about where you were when you took it. If you don't want to broadcast where you were for every selfie, think about turning off your location on your smartphone's camera.

CONNECTION

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.

Don't reply to messages that ask for your personal information — like passwords.

That's true even if the message looks like it's from a friend, family member, or company you know — or says something bad will happen if you don't reply. Chances are it's a fake, sent to steal your information. Just delete it.

Don't stay permanently signed in to accounts.

Log out when you're done using them.

Got apps? Try to check what information the app collects — before downloading. And check out your own privacy settings. Also think about whether getting that app is really worth sharing the details of your life. You might be giving the app's developers access to your personal information.

Check with your parents to make sure they're ok with you making in-app purchases, especially if they're paying for it.

PASSWORD TIPS

Passwords are one way to keep other people out of your accounts. Here's how to create good ones:

Be unique. Come up with different passwords for your different accounts. If you reuse the same password and it's stolen, someone could use it to hack into your other accounts.

Be strong. The longer your password, the harder it is to crack. Create a password with at least 12 characters. Use a mix of uppercase and lowercase letters, numbers, and symbols.

Avoid the obvious. When creating passwords and security questions, don't use names, dates, phone numbers, where you go to school, or anything someone could learn about you from social media. That's too easy to guess. Get creative! And definitely don't use "password123!"

Keep it private. Don't share your passwords with anybody, including your best friends, or your boyfriend or girlfriend.





WI-FI HOTSPOTS

Guess what? Many public Wi-Fi hotspots — like at libraries, coffee shops, and airports — aren't secure. And they may not protect your passwords, messages, photos, and account info that you send and receive.

Here's how to protect your information when using public Wi-Fi:

Turn off the Wi-Fi auto-connect feature.

That way you can choose which networks to use and when.

Look for a pop-up window asking for a WPA or WPA2 password. If you're not asked for a password to join a Wi-Fi hotspot, other people might be able to see what you're sending.

Use secure websites. Look for sites with a padlock symbol or https in the address. The "s" stands for secure.



Don't use apps that ask for personal information.

If your device is connected to a Wi-Fi network, your apps that use the internet will connect to that network, too.

PROTECT YOUR DEVICES

Be cautious about opening attachments or clicking on links. They may hide viruses or spyware that could mess up your device.

Password-protect your devices. It'll help prevent annoying "pocket-dials" and help keep your photos, messages, and accounts from falling into the wrong hands.

Whether it's your phone, laptop, or tablet, don't leave it in public — even for a minute.

IT'S FREE!

Is it really free?
What's the catch?

Sometimes "free" stuff — like videos, apps, games, or music — can hide viruses or malware. Don't download unless you trust the source.



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

WORD SEARCH

T T L N A S T S F 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 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

APPS
PRIVACY
RESPECT
DOWNLOAD
TEXTING
POLITENESS
PROFILE
VIRTUAL
SECURITY
SPYWARE





FTC.gov/OnGuardOnline 

To get free copies of this brochure,
visit **FTC.gov/bulkorder**.



STOP | THINK | CONNECT™

September 2016