Online Safety

How could we live without our smartphones, laptops, and other devices that allow us to go online? That's how most of us keep in touch with friends and family, take pictures, do our homework, do research, find out the latest news, and even shop.

But besides the millions of sites to visit and things to do, going online offers lots of ways to waste time — and even get into trouble. And just as in the non-cyber world, some people you encounter online might try to take advantage of you, steal your personal information, or harass or threaten you (called cyberbullying).

You've probably heard stories about people who got into trouble for something they did online — whether it was sending an inappropriate photograph by text message, joining in on some online bullying on a website or message app, or getting ripped off by someone they met through a website.

Because users can easily remain anonymous, some of the more popular websites and messaging apps might attract adults who pretend to be teens or kids. They'll sometimes ask visitors for pictures or information about themselves, their families, or where they live — information that shouldn't be given away.

Usually, the people who request personal information like home addresses, phone numbers, and email addresses use this information to fill mailboxes and answering machines with advertisements. In some cases, though, predators may use this information to begin illegal or indecent relationships or to harm a person or family.

Smart Surfing

First rule? Check your mood! Are you feeling upset or angry? Then this is not the time to be messaging or posting on a social media site. People don't always make good decisions or think straight when they're stressed out or upset. If you have to, call someone or go for a run instead before you start venting online.

Second rule: when you're on a website, try to remain as anonymous as possible. That means keeping **all** private information private. Here are some examples of private information that you should never allow the public to see:

- your full name
- any type of photograph (even of your pet!)
- your current location (some phones have automatic GPS apps built in that may need to be turned off)
- home or school address or the address of any of your family or friends
- phone numbers
- Social Security number
- passwords
- names of family members
- credit card numbers

Most trustworthy people and companies won't ask for this type of information online. So if others do, it's a red flag that they may be up to no good. Always check with a parent if you are unsure, especially when shopping online or signing up for a website or app.

Think carefully before you create an email address or screen name. Web experts recommend that you use a combination of letters and numbers in both — and that you don't identify whether you're male or female.

When using messaging or chat/video apps, use a nickname that's different from your screen name. That way, if you ever find yourself in a conversation that makes you uncomfortable, you can exit without having to worry that someone knows your screen name and can track you down via email. Some people who hang out with their friends online set up private chat rooms where only they and the people they invite can enter to chat.

Safety experts recommend that people keep online friendships in the virtual world. Meeting online friends face to face carries more risks than other types of friendships because it's so easy for people to pretend to be something they're not when you can't see them or talk in person. It's safer to Skype or video message with someone first, but even that can carry some risks. Check with a parent that this is a safe thing for you to be doing. They may want to meet some of your contacts or sit in on a conversation before they allow you to set up Skype by yourself.

If you ever get involved in any messaging or online chats that make you feel uncomfortable or in danger for **any** reason, exit and tell a parent or other adult right away so they can report the incident. You also can report it to the website of the National Center for Missing and Exploited Children — they have a form for reporting this type of incident called CyberTipline. They will then see that the info is forwarded to law enforcement officials for investigation.

Cyberbullying

It's not just strangers who can make you feel uncomfortable. Cyberbullying refers to cruel or bullying messages sent to you online. These might be from former friends or other people you know. They can also be sent anonymously — in other words, on a website where everyone has a screen name, so teens being bullied might not even know who is bullying them.

If you get these bullying messages online, it's often better to ignore them rather than answer them. Cyberbullies, just like other bullies, might be looking for attention or a reaction. Plus, you never want to provoke bullies. By ignoring them, you can take away their power. You also can try to delete or block bullies so you no longer see their messages or texts.

Fortunately, most people never experience cyberbullying. But if you're getting cyberbullied and ignoring it doesn't make it stop, getting help from a parent, school counselor, or another trusted adult might be a good idea. That's especially true if the cyberbullying contains threats.

Other Things to Consider

Although email is relatively private, hackers can still access it — or add you to their spam lists. Spam, like ads or harassing or offensive notes, is annoying. But spam blockers can keep your mailbox from getting clogged. Many service providers will help you block out or screen inappropriate emails if your parents agree to set up age-appropriate parental controls.

If you don't recognize the sender of a document or file that needs to be downloaded, delete it without opening it to avoid getting a virus on your device. Virus protection software is a must for every computer and should be updated regularly. You also can buy software that helps rid your computer of unwanted spyware programs that report what your computer is doing. Some service providers make software available to protect you from these and other online annoyances, such as blockers for those in-your-face pop-up ads.

When you're out and about with your devices, keep them secure. Don't let other people use your phone unless you're with them. Don't leave your phone where someone else might pick it up, and turn your laptop or tablet off when you're not using it. Don't make it easy for other people to get a look at your personal information.

Finally, remember that any pictures or text messages that you send could become "leaked," or public, as soon as you hit send. Think about whether the words you've written or the pictures you're about to share are ones that you would want other people reading or seeing. It's always better to be safe than sorry. A good rule is that if you wouldn't want your grandmother to see it or read it, you probably shouldn't send it or post it.

Reviewed by: Michelle J. New, PhD
Date reviewed: October 2014
