

How to Stay Safe on the Internet (for Kids)

If you're a kid who likes to use the Internet, you'll need to know how to stay safe while browsing. The Internet can help kids of any age with academics and social networking with friends, but it can also lead to dangerous situations if you don't follow the necessary precautions to take when surfing the web.



Part 1: Browsing Safely

1. Avoid responding to messages from strangers, in general. Just like you should never talk to strangers on the street, the same rule applies online. The person you're talking to online could be dangerous and using a fake identity.

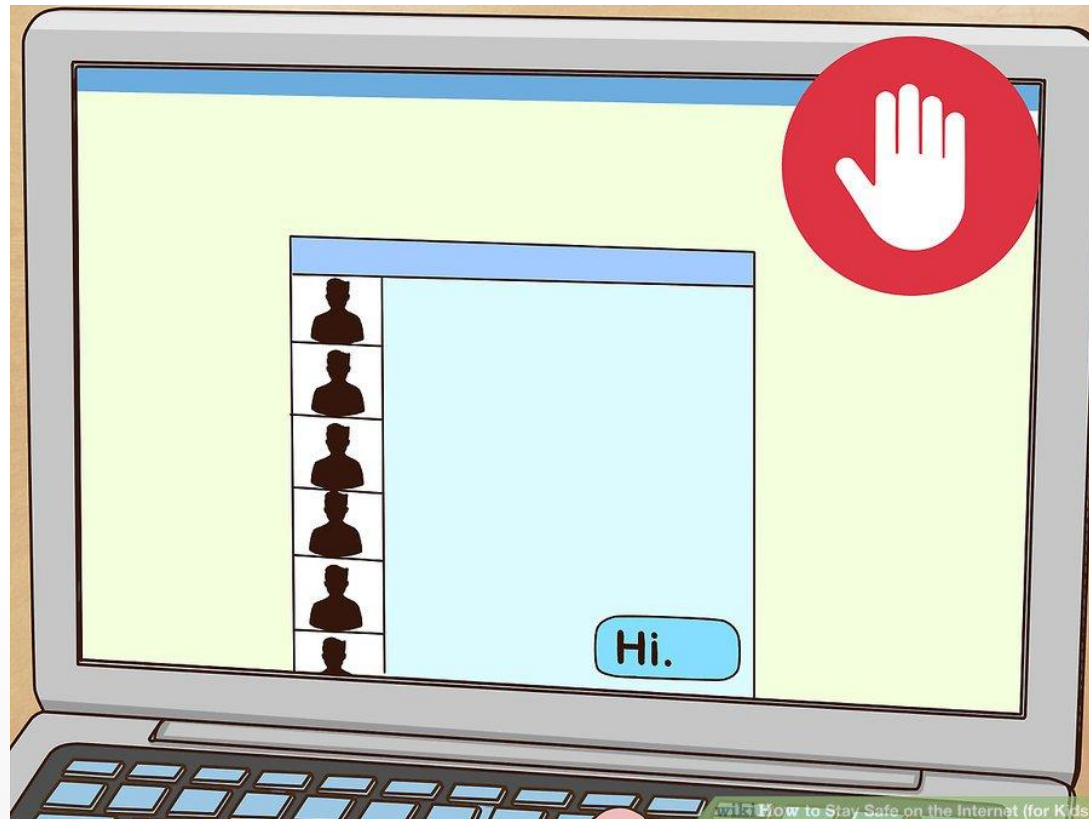
If you do decide to talk to a stranger online, be extremely careful. If the person seems to be who he/she says he/she is, trust cautiously and take things slow. Never reveal your address, age, your school, your grade level, your profession, etc. Be doubtful where you need to be and always be extremely vigilant for suspicious signs, such as someone you don't know asking you for money or sex.



2. Be careful when meeting with strangers. Even if you've been talking to the person for a while and have formed what you think is a trustworthy relationship, you still need to use a certain degree of caution. Always, always ask your parents for permission to meet up with this person and bring your parent or guardian along. Always meet up in a public place; that way, it is easier for police and authorities to catch anything suspicious. Never have your first meeting at either person's home; absolutely wait until you can trust this person enough before you do so



3. Avoid joining private forums and chat rooms. By entering a forum, you provide everyone there with your email address, which can be used to track down your address and personal information. Unfortunately, there are also adults out there that join forums and chat rooms in order to talk to kids. Adults should never use the Internet to talk to kids, and if they do, they likely have a dangerous reason for doing it, so it's best to avoid websites where this is common. Many adults are completely who they say they are, too, but it's best to know the signs.



4. Avoid going on dating sites. If you're a teen interested in dating, try starting with someone you know. Dating sites can be dangerous, as you don't know who you're actually talking to, their age, or their background. Sometimes adults pose as teens in order to take advantage of kids they meet on dating sites.

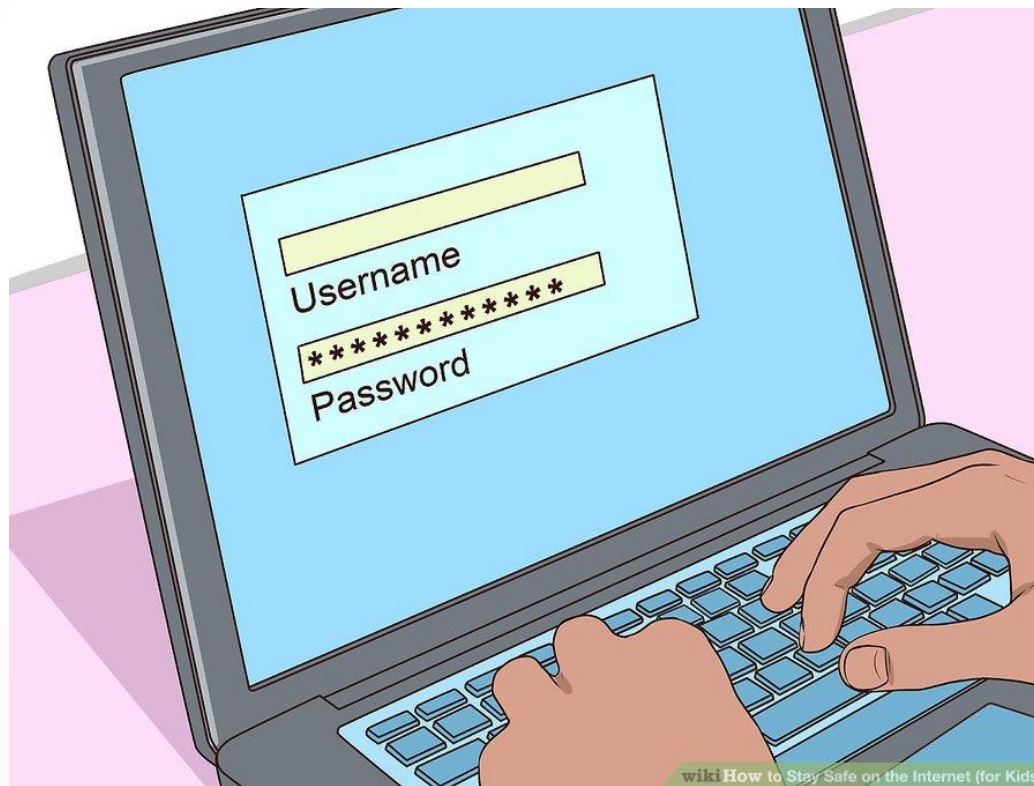


5. Avoid accepting random friend requests on social media. If you have a social media account such as Facebook or Twitter, don't accept friend requests from people you've never met before. They may be using a fake profile to hide their true identity, and often, online predators make friend requests to lure you into talking to them. Keep your friends list free of strangers and full of friends and family members.

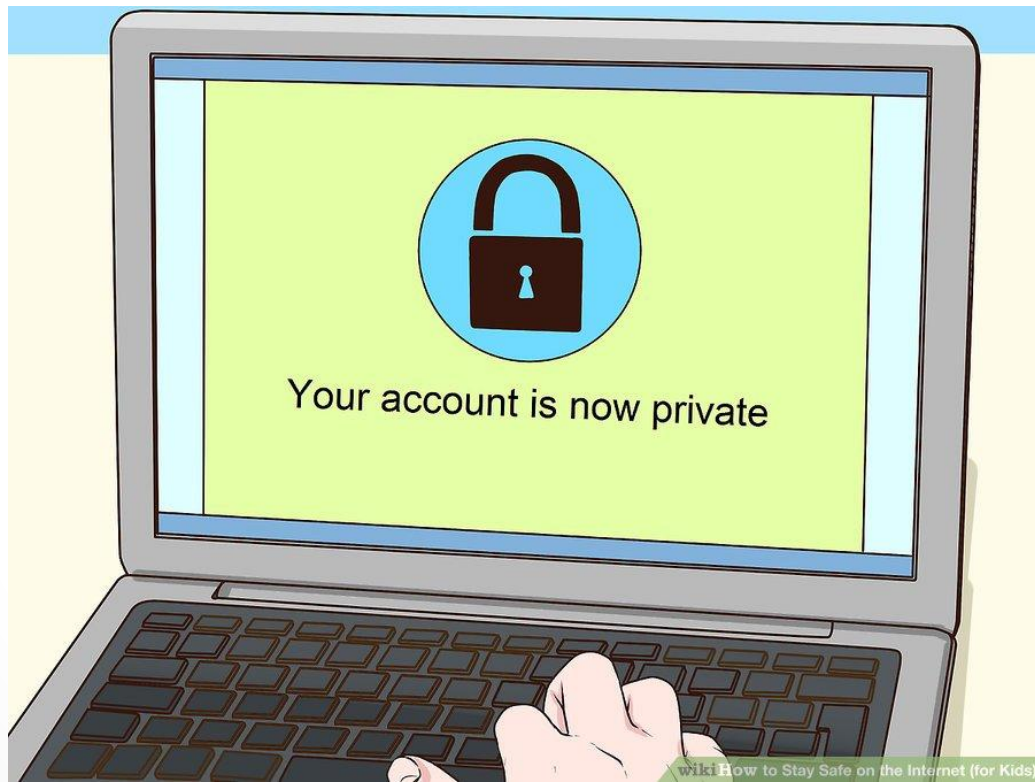


Part 2: Protecting Your Identity

1.Create strong passwords. Your password should not be something obvious like your favorite song or your pet's name. It should be a mix of random letters and numbers that would be difficult to guess. Use a different password for every site you log into, and change them every few months. Don't give out your password to anyone, including your best friend.



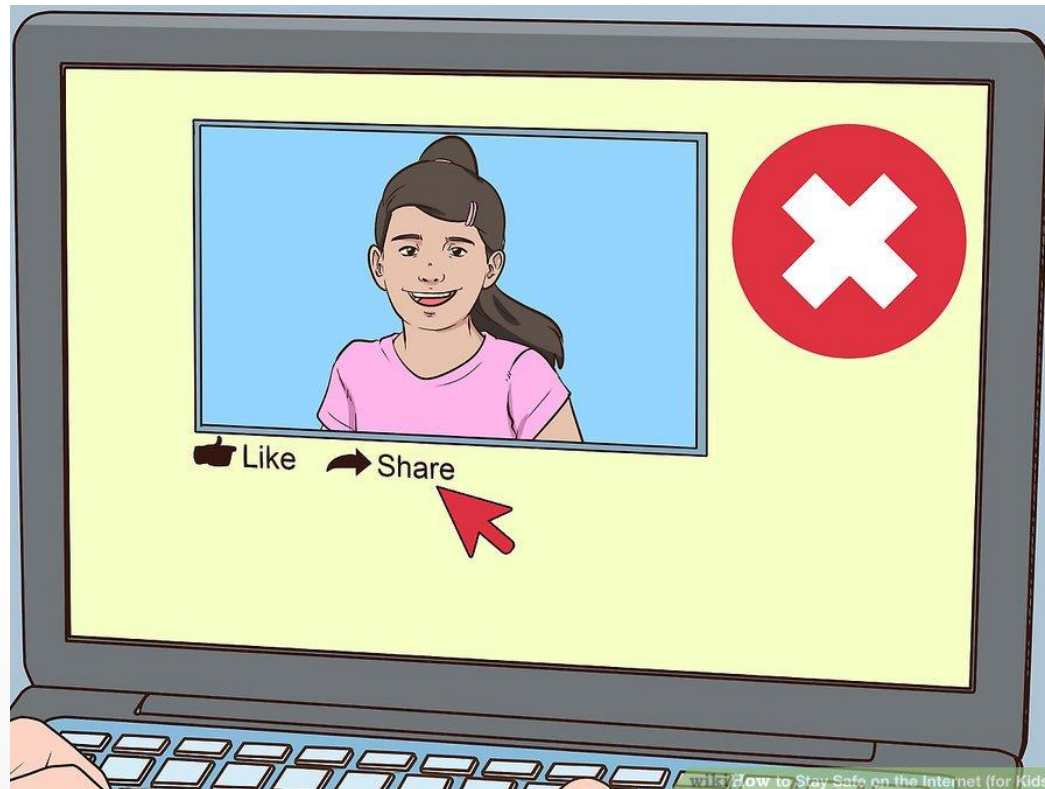
2. Set your social media accounts to private. Make sure your Facebook and other accounts are set to private, which means that only your friends can see your posts and photos. If you leave your account open to the public, strangers can view your profile and potentially learn personal information about you.



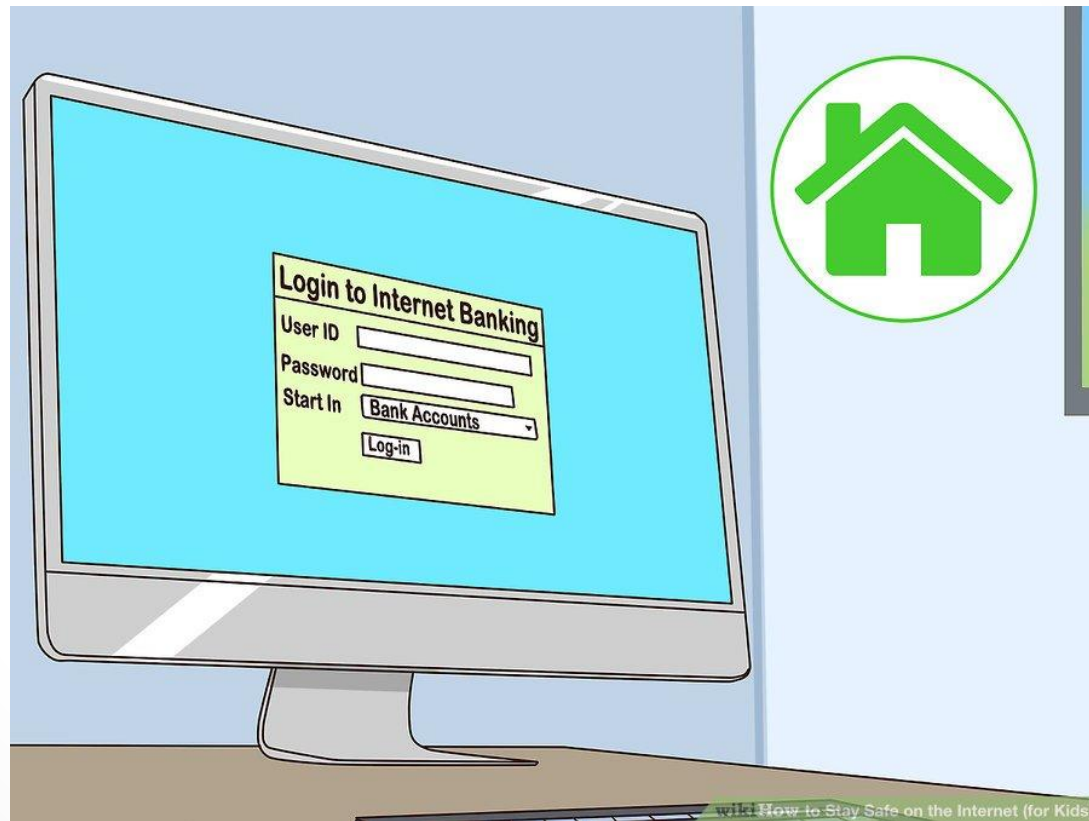
3. Avoid giving out your personal information. Don't give out your phone number or address to anyone online, ever. You also shouldn't share your social security number, the name of your school, or any information about your parents, family, or friends.



4. Avoid sharing personal photographs. Don't post photos of yourself if you're wearing clothes with the name of your school or town on them. Your personal photographs can also be used by others on their social media platforms to steal your identity. Just say "no" if someone asks you to send them a picture of yourself. You also shouldn't post photos of yourself by easily identifiable landmarks (such as the Empire State Building in New York or the Bean in downtown Chicago), or others may be able to find out where you are.



5. Enter private information on your home computer only. If you're using a computer in a public place or at your friend's house, don't go on any of your private accounts, such as your bank account. Save that until you get to your home device.



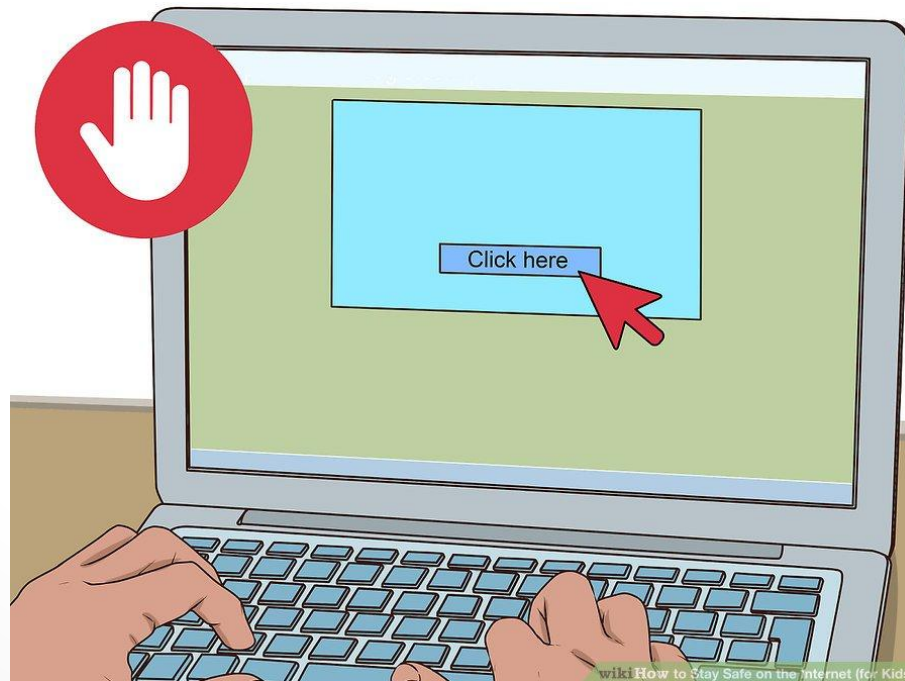
6. Avoid sharing financial information. Don't post pictures of money, checks, or credit cards because someone could see them and try to steal from you. Avoid sharing the name of your parent or guardian's bank or any financial information with anyone.



7. Disable location services. Many phones and social media sites automatically use location services. This means every time you post a status or photo, there will be a location tag attached to it that tells people where you are. If anyone on your social media can know where you are, that means that they can follow you. To disable location services, go to “Settings,” then “Privacy,” then “Location Services” and make sure it’s set to “Off.” Don't “check in” to places on Facebook or other social media platforms. Don't share when you are going out of town because people will now know that your house is empty.



8. Avoid opening spam. Spam consists of advertising, hoaxes, and malware. Avoid opening emails that promise large sums of money or prizes as well as those that ask for personal information. If you receive a message that says “hi” followed by your name, that doesn't mean that the person actually knows you. They can find out your name if it's attached to your email address. If you don't recognize the email address that sent you a message, don't open it. If you happen to open the email and notice something that says, “click here,” don't click it. It probably contains some sort of malware or computer virus.



9. Purchase items from reputable sites only. Don't buy something online unless you know it's a trusted site. Always ask your parents before putting in your personal information and making the purchase. You wouldn't want to get scammed out of your well-earned allowance!



10. Keep your virus protection updated. This will keep you safe from computer threats and malware. Viruses and malware can be used to steal your personal information or infect your computer with a bug that will damage it. You may have to ask your parent or guardian how install or update virus protection on your device.



Part 3: Reporting Dangers

1. Report anybody who makes you uncomfortable. Tell your parents when anyone online has made you feel uncomfortable or said something inappropriate to you. This includes strangers or people you know. For example, if a stranger keeps pestering you to send them photos of yourself, tell your parents right away.



2. Block cyberbullies from your social media accounts. Unfortunately, some people use the Internet to bully others. They may make fun of you or even threaten you. The best thing to do when you come across a cyberbully is to block them from your accounts. On Facebook, Instagram, and Twitter, go to their profile and click the “...” button toward the top of the page. This will display a dropdown menu where you can click “block.”



3. Report cyberbullies. If the bully continues to try to contact you from another account, tell your parent or guardian immediately and don't respond to the cyberbully in any way. If the bullying has gotten out of hand, it may have to be reported to your school or the police.



4. Report online abuse. Social media statuses can erupt into arguments in the comments sections. Keep your opinions to yourself, and don't join in on the argument. If you see someone else getting bullied or stalked online, report it to your parents so they can call the police and fill out a police report. Don't be a cyberbully. An online bully could be putting themselves in danger, because bullies tend to get negative responses from Internet users. The lesson here: online bullying is dangerous whether you're the bully or the victim.



5. Use the “report” button. Many social media sites offer a “report” button that you can click if someone's comments seem inappropriate. If someone is sending you comments that make you feel uncomfortable, press “report” and then be sure to block that user. For example, report someone who uses swear words or inappropriate language or photos.

