Internet Safety Tips for Tweens & Teens

The internet is a ton of fun! It's where you and your friends can hangout and play games together, watch silly YouTube videos or make creative TikToks. But the internet can also be kinda scary if you don't know how to be careful about it. Don't worry though we have tons of tricks to keep yourself and your friends safe online.

Safe Browsing:

Googling can help us learn so much, we can go anywhere we want or let us read and watch anything we want. Sometimes this can cause us to end up on websites that aren't very good. These bad websites can be really appealing to visit because they might offer us free gear for a favorite game, to watch a movie we really want to see before it's even come out or they might scare us by claiming to know a secret about us.

Once we are on these sites and clicking on links they can do all kinds of damage to our computers and other devices. They can put viruses on our computers, take private information from us like our addresses or our parent's credit card information and use that information for whatever they want. It's almost like letting in the bad guys and handing them all the information they need to make their crimes easier to get away with.

So how can we be sure we are on a good website or a bad website?

There are lots of clues websites will give you whether they are good websites or bad websites. One of the first clues is in their address. All websites have addresses like houses do. Most websites will end their address in either a .com, .org, .edu, or a .gov. These websites are telling you that they are safe to visit. Bad websites will look very similar to a good website but they will change the ending of their address so it might look like .co, .ogr. .eud, or .gbo. Their addresses look really close to real ones but there is always something off about them.

Another great clue is to look for the lock. Kinda like how we lock our houses, good websites will lock their doors from bad guys too. When websites have a lock on them they are telling you they are encrypted or that they are protecting your data and information from people who would want to steal it. Online shopping sites as well as email and cloud services will have this symbol.

Another clue is there at the very start of the website, when you see the https:// at the start of the web address. While not every good site will have this no bad website will. The 's' stands for security which means the website is letting you know that it is taking precautions to protect you from viruses and people that would steal your information.

If a website you are visiting asks for a credit card number or asks you to download anything leave the website and tell an adult! While sometimes these requests are okay and safe they aren't always. Those download links can put viruses and other nasty things onto a device and by giving them a credit/debit card they can then use that information to take all your or your parents' money!

Privacy and Social Media

Websites like Twitter, SnapChat, Instagram and TikTok can be great ways to connect with your friends and meet new people but they can also be dangerous if you share too much with people.

Things like your address, what school you go to, who your family members can be used by people who pretend to be your friends to hurt you. So you want to make sure you never share that information on any of your social media.

One of the ways these bad people will use your information is to catfish you or they will pretend to be someone they aren't. They can use your age and school to create a fake account where they will appear to be the same age as you and that they live close in order to trick you into adding them only for them to turn out to be an adult. These adults will pretend to be a kid like you and get you to share all sorts of secrets and information with them and then use it to find you, bully you or hurt you in other ways. Which is why you must only add people you know in real life. Your family members, or kids from your school. If you don't know someone who is friend requesting you ask an adult about them or just ignore their follow request.

Some ways you can protect yourself is to make sure to keep your accounts private, make sure people have to ask you permission to follow you. And make sure you don't use location tagging or have your location turned on, on your devices some apps like SnapChat will automatically turn on location and show people where you are at.

How to Spot a Fake Account

Fake Accounts can be tricky to catch. But if you know what to look like you'll be catching them every time they show up! On Twitter their screen names will usually be their first name and last name and a string of numbers they will be following a large number of people but have no followers at all.

On Instagram they will also be following a large number of people with very few to no followers and only have maybe one or two posts that look like they could be fake pictures or pictures they stole from someone else.

On YouTube they will comment, things like let's be friends or great content wanna collab? They will also use an avatar picture rather than their own picture. Their comments will never mention anything about the video or your comment in theirs. It will always be very generic and feel like they comment that a ton of times a day.

You can also reverse image search to see if they are using a real photo or if they took someone else's. If you copy and paste or drag the image over to Google's image search google will look for the picture and you can use that to see if it links to other accounts with that name, or if it shows up on someone else's page. This is also a great way to check to see if an image has been doctored or photoshopped as well when it comes to the news!

Passwords and Security

Passwords are like locks to your online accounts. They keep your information safe from nosey people like a lock on a house. But you need to make sure they are strong, like really strong! So what does a strong or weak password look like?

A password should never include your date of birth, your street name, a name of a pet or a hobby. So using my pet's name as an example and my birthday, a weak password would look like kennedy1990.

If you noticed it's also all lowercase which isn't good either. That's really easy to guess. A strong password will be a mixture of capitalized letters and lowercase letters, numbers and be made up of multiple words.
For example (please not use this password for your own!)
tH3quiCKr3dF0xjuMPEDOVErthe!AZYBRowNd0g

If you noticed some of the letters were switched with numbers and randomly capitalized, I also used a sentence rather than just a couple words. A password can be made even stronger though by including symbols as well.

When you make passwords like my strong example that makes it harder for computer programs designed to guess passwords to guess yours because it has to run through letters both lowercase and uppercase, numbers and then symbols as well.

Trolls in the dungeon and other mean people

Have you ever heard the phrase "don't feed the trolls" or "internet troll"? These people and sometimes bots(computer programs that can sometimes seem like people) are out to start fights with people on the internet. They will say some of the meanest things you've ever seen and this is all to get your and everyone else's attention. Sometimes they attack people personally or they will say things about current issues or groups of people that they know will upset everyone.

The best way to deal with a troll is to not feed it or to ignore and report them. If they keep trying to start a fight with you even after that, it might be a good idea to also block them.

If you see someone threatening violence though first tell an adult! These posts have to sometimes be reported to authorities if they mention specific plans and locations they are planning on attacking. These posts have to stay up so that police and other law enforcement can track their IPs or their computer's address to find out who the person behind the screen name is.

Not every mean person you meet on the internet is a troll though, sometimes they are just a bully which looks a lot like a troll only you probably know they bully. They are only targeting you and are spreading rumors about you online, sharing pictures of events your friends are at but you are invited to, and insulting you.

If a classmate or other person is bullying you online tell an adult! Your parents, a teacher, the principle.Talk to any adult you trust so that they can intervene so that the bullying is stopped.

What if you are accused of bullying and being a troll? How do you prevent those accusations? We all can be mean even if we don't mean to be. If someone tells you you are trolling or bullying them, apologize. That's the best way to stop being a bully or a troll and then make sure to be nicer next time.

A good rule of thumb though when talking to people online is to only say what you would say to that person to their face. If you wouldn't say it to their face then it's best to not type it.

The internet is a great place that allows people to learn anything and be anyone but that is what makes the internet bad too. It's easy to be meaner than you normally would be if you can hide behind a fake picture or pick any name you want.

Online Gaming

Whether it's gaming on a computer, xbox live ,playstation plus or now or another online gaming platform is a great way to pass time. It's a ton of fun for everyone to hunt monsters, race cars or create whole worlds. The ability to play with your friends and strangers is also what can make online gaming risky. It's impossible to know who you are really playing with.

Which is why you should be careful what you and your friends say so you don't accidentally give away identifying information much like you wouldn't on social media or out around town.

It can also be tempting to trash talk when fights and games get intense but if you wouldn't say the insult to their face it's probably not a good idea to say it over voice chat. And if someone is getting really mean with you in voice chat either leave the match or if it's threatening tell an adult and leave the match! No one should ruin your fun in a game just like you should make sure you keep the game as fun as you can for everyone!

Beware of trades and in game purchasing as well. If someone is offering to trade you a super rare piece of gear or loot for yours think twice about going through it. A lot of times if you don't know the person offering the sale or the trade they are not out to actually trade with you but rather to trick you and take your gear or loot for themselves and leave you with nothing.

Online Shopping

Online shopping is really fun and convenient, with just a couple pushes of some buttons everything from snacks to games can be sent right to us. It's important to be careful and aware of how easy online shopping and in app purchases can be though.

Sometimes because it's so easy to buy things it doesn't even feel like you are actually paying for anything which can cause the charges on your or an adult's account to quickly add up and cause trouble by having too much money taken out of an account when that wasn't really the plan.

Which is why it is always important to ask an adult if it is okay to buy something in game or off a trusted website like Amazon or other online stores as well as app stores on devices like your xbox, playstation or tablet.

It's also important to check with an adult in case it turns out a site isn't safe to buy from. Like when we discussed why it's important to not enter in a credit or debit card if a site randomly asks for it, buying from an online store that isn't safe can cause very similar problems from money being taken out of the account that no one agreed to or personal information like addresses being stolen and used to cause harm.

The internet is a really great place that lets us have fun and learn anything we want and hopefully after reading this you'll feel really good about being on the internet and how to safely navigate any situation that might come up!

Never DO/ Tell an adult

Bullying or Trolling
Sharing private information
Giving out passwords or credit/debit card numbers

Ask First

Online Shopping
In Game Trades
Sites that don't have the https://

Always Safe

Asking adults for help.
Being friendly and kind online
Only talking to people you know
Visiting secure websites

Want to know more? Read these books!

A Smart Girl's Guide. Digital World : How To Connect, Share, Play, And Keep Yourself Safe By: Carrie Anton

Learning About Privacy by Martha E. H. Rustad

Safe Social Networking by Heather E. Schwartz