ON THE GRID

Social media can be a great tool to keep in touch with friends, share memes and read about news in your community. As with any online activity, though, you should stay smart about how you use social media. If you know the risks of social network sites and follow the safety tips in this brochure, you'll be a safer digital citizen.

CYBERBULLYING

Cyberbullying usually happens on social media websites and gaming platforms through private messaging and content posts. Posting someone's personal information or sharing mean, embarrassing or untrue content on social media with intent to harm or make fun of someone is cyberbullying. Cyberbullying hurts people and in many states is a serious crime.

Even online, you should always act the way you would when talking to someone face-to-face. A good rule is to never post anything that you wouldn't feel comfortable saying onstage to a crowded room. Remember to be polite and kind - everyone on the internet is a real person. Since people can't hear your tone of voice on the internet, be careful how you word your posts. If you think you or someone you know is being bullied online, let your parents or a responsible adult know.

CHILD PREDATORS

Child predators are adults who try to get young people involved in harmful sexual activity. The anonymity of the internet makes it easy for these dangerous criminals to hide and socialize.

When online, child predators can lie about their identity by using fake pictures and names. It's common for these criminals to contact victims on social media and lie about their age, gender and other details to establish relationships with minors. A word commonly used to describe luring in someone with a fake online persona is "catfishing." Catfishing is another way of "grooming" victims; grooming is the practice of preparing a child for an in-person meeting with the predator, so that the predator may sexually assault or otherwise harm the child.

> **"SOCIAL MEDIA IS ALSO HOME TO PREDATORS LOOKING TO TAKE ADVANTAGE OF VULNERABLE PEOPLE."**

Child predators can use the Internet to gather information about their victims. They might look for a child's hobbies, interests, school, or friends - anything that would help them start a conversation and build trust. All of these details help them create a convincing persona that a child may want to meet. Sometimes they may even impersonate people you know to get close to you.

To stay safe from child predators, never agree to meet someone alone after meeting them online. You should make sure your parents or guardians are aware that someone you've met online is trying to meet you in real life. Never share pictures or important personal details with someone you haven't met in person, as you can never really know what a stranger will do with that information. If your only contact with someone is through their social media profile, you don't have any way to be sure that they are who they say they are.

ADDITIONAL RESOURCES

US Government Internet Safety Site

usa.gov/online-safety

"Your Life Your Voice" Hotline

Call 1-800-448-3000 [Available 24/7]

Text VOICE to 20121 [12 noon to 12 midnight CST] (Free with most major carriers)

Or visit yourlifeyourvoice.org

Anti-Bullying Resource

stopbullying.gov

in the know

SOCIAL MEDIA

Stay Safe Online

ONLINE SECURITY THREATS

Advertisements

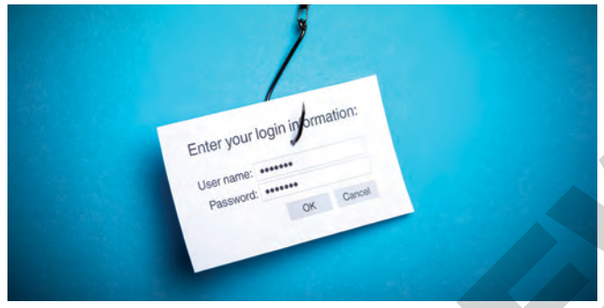
Social media sites and other websites track your information and online activity and sell that data to companies that want to create advertisements targeted towards you. Social media platforms use details that you share on your profile, like age, gender, location and interests to get an idea about what type of advertisements may get your attention.

Getting you to click on advertisements or any unfamiliar links is a common way for hackers and scammers to infect your computer or device with malware. Malware is software that is designed to disrupt, damage or gain access to your technology and personal information. Once your device is compromised and your information is stolen, it could end up in the hands of dangerous criminals.

Always be cautious about information that you share on the internet. If you post details like your phone number, street address, or credit card numbers, you leave yourself open to identity theft. This doesn't mean just content you post on your public profile. Private messaging apps on social media platforms aren't actually private and can collect your data, too. Experienced cyber criminals only need to collect a small amount of information about you in order to steal from you or harm you. If you need to give someone else personal information, do it in person or in a phone call—not on a social network site.

Phishing

Phishing is a cyber-crime that happens when someone poses as a different person or a legitimate company to get valuable data like passwords, credit card numbers or contact information. Phishing commonly happens through email and instant messaging on social media. Cyber criminals may use the accounts of your friends or trustworthy companies to contact you. They will often try to trick you into typing your account information into their fake websites, or to convince you to send them the information directly. A way to avoid phishing is to never send your personal information to anyone online or click on links from emails. The only people you should trust with your passwords or account information are your parents.



SAFE NETWORKING

The Internet can be a dangerous place, but you can stay safe by following these tips:

Keep Your Parents Involved

Don't be afraid to talk to your parents or a trusted adult (teacher, counselor, guardian) about your internet activity. When your parents know who you're talking to and what you're posting, it's easier for them to help keep you safe. If you ever feel uncomfortable, sad, scared or worried about something that you saw or experienced on the Internet, let your parents know. If you don't want to talk to your parents, use the "Your Life Your Voice" hotline listed in the "Additional Resources" section.

Know Your Friends

Never send or accept a friend request on social media to someone you don't know in person unless you have permission from one of your parents. Never meet someone in person that you met online unless your parents approve and will go with you.

Watch What You Share

Never share personal information or send private pictures or videos to someone online, even if you know them in person. Some examples of information you shouldn't share are your full name, the name of your school, your address, phone number, passwords, social security number, your birth date or your plans. Avoid posting pictures that show your current location or places you often visit. Some things that might reveal your location or information in a picture are streets signs, business signs, product logos and license plates. Avoid geotagging (pinpointing your location with a GPS tag) on photos or posts.

Usernames and Passwords

Never use the same password for all your accounts. Each password should include numbers, capitals and special characters. Never use words that are easy to guess or find out, like your name, birthday or popular phrases. Don't create usernames with your full name or any other personal information. No one should know your password except your parents. Remember to log out of your accounts when you're done with them.

Report Wrong Postings

If you find something inappropriate, dirty or hurtful on social media, report it to the moderators on social media sites. Usually the report is anonymous, so you don't have to worry about a person finding out that you reported them. After reviewing the complaint, the moderators decide whether the content violates their policies and punish them accordingly. Most social media websites have policies that ban inappropriate or abusive content, like harassment, threats, violence, graphic images/videos and scams. If you feel like you need to report something, tell your parents.

Maintain Your Digital Footprint

Remember, everything you post on the Internet is permanent, even if you "delete" it. Don't post or send anything online that you wouldn't want all of your friends, family, teachers, future employers or strangers to see.

Stay Secure

Do not reply, click on links or open attachments from an email or private message that looks suspicious. Signs of suspicious messages or phishing scams are aggressive or attention-seeking language like "immediate response required" or "you'll never believe this!" Another characteristic of phishing scams are poorly worded messages, grammar mistakes and spelling errors. Be cautious of messages asking for personal information or money. Make sure all of your devices are using up-to-date software. Don't open messages from people you don't know. Also, do not use public WiFi networks, especially if they aren't password protected.

Overall, follow your intuition! If something doesn't feel right, let a trusted adult know!

"Cyber criminals may use the accounts of your friends or trustworthy companies to contact you."