LEARNING RESOURCES

Keeping Your Family Safe on the Internet

Internet Safety for Children

The Internet is a wonderful place to find information and connect with people and friends. It does pose safety and privacy risks, though, especially to minors.

What you can do to protect your children online:

- Talk about Internet safety as soon as they begin using the Internet. It is never too early.
- Consider placing the computer in a common area of the house.
- Stay involved in their online world by monitoring with whom they email and chat. Get to know the websites they're visiting.
- Know their usernames and screen names and make sure they are appropriate.
- Use safe search engines. For younger kids in particular, use age-appropriate filtering and monitoring software.
- Educate yourself about computers, the Internet and potential risks to children online.

What your children should not do:

- Tell your child to never share their passwords with anyone, including friends.
- Teach them not to fill out forms without your knowledge, or open emails from strangers.
- Do not allow your child to go into private chat rooms.

Social Networking

Social networks have become very popular among adults and children alike. These sites allow users to communicate and share information. They can be accessed anywhere there is an Internet connection, including on smartphones.

The basics on some popular social networks:

- **Facebook** is a free social networking site used by people all over the world. Its policy requires users to be at least 13 years old, but many younger kids join by pretending to be older. By default, adults' posts are public; kids' posts can be seen by friends of their friends.
- **Twitter** is a real-time information network where people get the latest news, ideas, and opinions about what interests them. There's no age limit. Tweets are public by default.
- **LinkedIn** is a social site that allows professionals to network with business connections, search for jobs and hiring managers, join groups, etc. Users need to be at least 18 years old. LinkedIn users have a private and a public profile, the visibility of which they can control.
- **YouTube** is a free video sharing site and social network. Anybody can upload, watch and share videos on YouTube.

If your child wants to use social networks, talk to them about your expectations: how they should behave; what is safe and what isn't; when they can go to the site and how much time they can spend there (yes, social networks can be addictive).

How to protect your children's privacy and reputation:

- Go through Facebook's privacy settings together and select levels you're both comfortable with. Encourage your children to require their approval before they can be tagged in posts (one of Facebook's privacy settings). Set Tweets to be protected (private) by default.
- Teach them to never post personal information such as addresses, phone numbers, or where they are. The same goes for their friends' information.
- Discourage the use of webcams. Tell them to never send any image or video to a stranger. Under no circumstances should they upload a photo that contains nudity (it's illegal).
- Most importantly, teach them online common sense: think before you post or tweet. Would you want the entire school to see this post, photo, or video? If you would not say something to someone's face, do not say it in an online message.

How to protect your children's safety:

- Teach them to only accept requests from Facebook friends and Twitter followers they know personally ("Don't talk to strangers").
- Instruct your children to never agree to meet face-to-face someone they only know online.
- Keep lines of communication open. Your kids might not tell you everything, but that doesn't mean you shouldn't ask.

LEARNING RESOURCES

Keeping Your Family Safe on the Internet

Cyberbullying

Cyberbullying is using the Internet to harass or bully someone, for example, by spreading false rumors or sharing inappropriate images online.

How to prevent cyberbullying:

- Speak with your children about what is appropriate to say and do online. Be kind online.
- Review your child's online information from time to time. Seeing what others say on your child's pages can help you stop cyberbullying.
- Try to spot changes in your child's behavior that might suggest cyberbullying such as avoiding computers or appearing stressed when receiving an email or text.

What to do if you feel your child is a victim of cyberbullying:

- Tell your children not to respond to cyberbullying, but to stop, block and tell. 1) Stop interacting with the bully. 2) Block the bully from sending any more messages. 3) Tell an adult they trust.
- Document everything. Save emails and other communication.
- Seek help. If you feel your child is in immediate danger, report the incident to law enforcement immediately. You also may contact the Comcast Security Assurance Hotline at 1-888-565-4329.

Protecting your identity

Using strong passwords protects your valuable personal information and keeps you safe.

Password Do's and Don'ts:

- Do use a mix of letters, symbols and numbers.
- Do not use sequences (123 or abc) or personal information such as your birth date.
- Do not use easy dictionary words.
- Do not reuse old passwords.

Install Constant Guard™ Protection Suite and add your banking / shopping accounts to help prevent them from being stolen by hackers.

Email "Phishing"

This is when scammers send emails that pretend to come from a real company to try to trick you into revealing private information, like addresses or account numbers.

How to avoid Phishing:

- Don't reply to messages that ask about personal or financial information.
- Check the link: If you do not trust the website or sender, DO NOT click on any links in the email.

Spyware and Viruses

This is when a computer program gathers your information without your knowledge or permission. Spyware can make your computer work poorly (slow browsing, program crashes, etc.).

How to reduce Spyware:

- Install Constant Guard™ Protection Suite and activate Norton™ Security Suite.
- Be careful when visiting file-sharing sites (Gator, Kazaa, Hotbar, and LimeWire).

Spam

Junk email. This is when companies send emails to many people without permission.

How to reduce email spam:

- Keep your Norton Security Suite up-to-date.
- If you get suspicious emails, delete them immediately – do not respond.

If you need to give an email address to someone you don't trust, create an additional address. Take advantage of the additional email addresses Comcast offers you with your service.

For more information please visit InternetEssentials.com/learning or call 1-855-8-INTERNET (1-855-846-8376)

comcast