# Protecting Minors from Online Dangers

*by Sophia*

WHAT'S COVERED

Individuals, businesses, and organizations all utilize the Internet, due to its value as a resource for sharing information, communicating, and many other things. Unfortunately, there are also risks associated with Internet usage, such as exposure to inappropriate content, privacy, and cyberbullying. These risks are only greater when the person using the Internet is a minor. Being aware of the risks of using the Internet can be very helpful in staying safe while online. In this tutorial, we will identify potential online dangers, and some procedures for keeping minors safe online.

Our discussion will break down as follows:

## 1. Online Dangers

There are many potential risks for minors when online. Often times while exploring a website or social media, children will be confronted with vulgar content, such as inappropriate language. Furthermore, the potential exists for children to be exposed to pornographic content. Listed below are some common online dangers.

| Online Danger | Characteristics |
|---|---|
| **Phishing** | Scam in which a user is tricked into providing personal information. Usually involves an email, website, or online form that appears to be from a legitimate source (bank, government institution, etc.) soliciting a user for personal information. |
| **Cyberbullying** | Online bullying that takes place via social media, message boards, forums, and email. Cyberbullying usually refers to online bullying of children and teenagers, but anyone can be a victim. Those who would bully others face-to-face are likely to bully others online as well. However, due to the distance/lack of physical connection between a cyberbully and their victims, some people, who might not bully someone otherwise, are emboldened to bully others online. |
| **Cyberstalking** | Online harassment that usually involves the communication of threats online through social media, forums, email, and message boards. Cyberstalking is similar to cyberbullying, but the main difference is that cyberstalkers are unusually obsessed with their victims, and seek to collect any information about them. |
|  | Malicious software used to launch attacks on a computer system. Some attacks include |

© 2023 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

| | |
|---|---|
| **Malware** | malicious software that is designed to steal personal information from users; examples of malware include Trojan horses, worms, and viruses. |
| **Inappropriate Content** | Term used to describe posting text messages, videos, and photos that may be inappropriate for certain situations or age groups, i.e., children, professional situations. |
| **Web Sites and Chat Rooms** | As websites are the primary vehicle through which information is delivered online, children must be shown how important it is to protect their personal information and the information of their family and friends. Many child-oriented websites solicit information from kids in surveys and forms in exchange for prizes, and get them to register online for fan clubs. In chat rooms, sharing their gender, age, and favorite hangout could seem harmless, but predators can easily use this information to locate and harass the child. Predators may even masquerade as children in order to gather information, and ultimately meet their unsuspecting victims. With websites and chatrooms, the potential does exist for kids to pretend to be older than they actually are, not thinking about the potential results of such actions.<br>Chatrooms and online forums are typically where children get into online fights or become the target of bullying via email, chat, and instant messaging. |
| **Blogs and Social Networking** | Blogs and social networking websites such as Facebook, Twitter, Instagram, SoundCloud, and YouTube are places where children sometimes share too much information — not only names and addresses, but also personal photos that sometimes show illegal acts, such as underage drinking. Minors should be instructed to share their blogs or online profiles with a parent or guardian so content can be filtered for appropriateness. You can also use Google, along with the search tools on social networking sites, to search for profiles your child may have posted. Use your child's full name, phone number, and other identifying information. |
| **Peer to Peer (P2P) File Sharing Software** | Peer-to-peer (P2P) file sharing invites new privacy problems. These types of programs allow people to browse and download files from Internet-connected personal computers of anyone else who uses the same program. This makes it easy for cybercriminals to spread viruses, Trojan horses, and spyware. Children can also accidentally download inappropriate content, such as pornography, that is labeled misleadingly. |

# 2. COPPA and CIPA

As the popularity of PCs increased and the Internet evolved, the need to protect minors utilizing the Internet became increasingly evident. To do this, the U.S. government drafted legislation to address the access that children would have to inappropriate content, as well as legislation to address websites that collect information from children.

- **CIPA**: The **Children's Internet Protection Act (CIPA)** requires that public schools and organizations receiving Internet service at a discounted rate (through the federal E-rate program) provide an Internet safety policy that contains information as to how minors will be protected online. Specifically, CIPA requires that any obscene or pornographic pictures be blocked or filtered, thereby restricting a minor's access to harmful content. CIPA also requires that entities subject to CIPA have a hearing or forum to notify the public of its Internet safety policy.
- **COPPA**: Websites that are collecting information from children under the age of 13 are required to comply

© 2023 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

with the **Children's Online Privacy Protection Act (COPPA)**, which is enforced by the Federal Trade Commission (FTC). To comply with COPPA, organizations must make a good-faith effort to determine the age of those accessing their websites. If users are under 13 years old, organizations must obtain parental consent before collecting any information.

TERMS TO KNOW

**CIPA**

Short for Children's Internet Protection Act; requires public schools and organizations to block or filter pictures that may be obscene or pornographic in nature.

**COPPA**

Short for Children's Online Privacy Protection Act; requires parental consent before collecting information from people under 13 years old.

# 3. Online Safety Tips

- **Learn the Online Dangers**: Knowing the pitfalls prior to your encountering them will help to make your online experience more effective, by increasing the time you have to be productive. You will also be better prepared to talk to children about the online dangers.
- **Set Rules to Govern Computer and Internet Usage for Children**: Establishing rules for computer and Internet use sets behavioral expectations in the same way that an AUP does for employees and guest users. It is also important to set limits for when children can use the Internet. By not allowing children to use the Internet at night, or when responsible adults are not present, children are less likely to intentionally or unintentionally put their safety at risk. Monitoring software is also available to help monitor Internet usage of users when you are unable to physically monitor online use.
- **Explain the Importance of Maintaining Personal Information**: To keep criminals away from you or loved ones, it is always a good idea to keep your personal information private. Posting your personal information on websites or social media can give criminals access to it.
- **Understand How to Use Social Media**: Understanding how to use social media sites such as Twitter, Facebook, and Instagram can help you to avoid the pitfalls with regard to how people interact on them. These sites tend to be very popular with children and teens. Often social media sites will require personal information from their subscribers. Minors should guard their passwords, and never post personally identifying information or inappropriate photos. Blogs and social networking sites offer privacy tools that can be turned on to restrict potentially dangerous users. The sites automatically provide these protective tools to kids under 15. Kids should share information only with people they know from the real world. It's imperative that your kids let you know if they arrange in-person meetings with people they meet online. Before any such meeting, you should confirm the person's identity, and you should accompany your child to the meeting in a public place. When using P2P file-sharing programs, kids should not download files from users whom they don't know. They could be downloading infected files, pictures, games, and music that are inappropriate, or media files protected by copyright law. Don't allow kids to fill out online forms or surveys.
- **Malware Protection**: Installing anti-virus and anti-malware software is an effective way to keep your computer safe from malicious software that can cause harm to your computer. This software automatically scans email attachments and other downloadable files for viruses before they are downloaded or installed on your computer. Some malware protection software can also filter inappropriate content and

© 2023 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.

block access to sites that might expose minors to graphic content and online predators.

## SUMMARY

It is important to be safe while **online**, as there are a number of **dangers** to both minors and adults. Knowing the risk associated with the Internet can be the best way in which to defend yourself and your information from malicious attacks. In this tutorial, we discussed the potential threats that exist for online users. We also discussed ways in which to **keep minors safe** while online.

Source: Derived from Chapter 12 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity. https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html

## TERMS TO KNOW

**CIPA**
Short for Children’ Internet Protection Act; requires public schools and organizations block or filter pictures that may be obscene or pornographic in nature.

**COPPA**
Short for Children’s Online Privacy Protection Act; requires parental consent before collecting information from people under thirteen years old.

© 2023 SOPHIA Learning, LLC. SOPHIA is a registered trademark of SOPHIA Learning, LLC.