From Both Sides:

A Parental Guide to Protecting Your Child's Online Activity

CIS Center for Internet Security®

Contents

Introduction

In the vast ocean of the internet where tides of information ebb and flow endlessly, our children stand on the shorelines, curious and eager to dive into its boundless possibilities. But just as the sea conceals treasure and peril, the digital world offers knowledge and opportunity alongside risks and dangers. *From Both Sides: A Parent's Guide to Protecting Your Child's Online Activity* is crafted to help parents and guardians understand these risks, specifically the hazards of harmful online behaviors and scams targeting children. It also provides the essential tools to guide young surfers safely.

In the following chapters, my daughter and I will explore real-life scenarios that illustrate the common online pitfalls children may encounter. From cyberbullying to predatory behavior, privacy breaches to phishing scams, each scenario is dissected to uncover the ways in which these situations arise, their potential impact, and methods to prevent and manage them. Through these stories, parents and guardians will gain insights into the subtle signs that may indicate a child is at risk and learn proactive strategies to help their children navigate the internet safely.

This guide does not propose shielding children from the internet altogether; instead, it aims to empower parents and guardians with practical knowledge and strategies. By understanding the nature of online risks and equipping children with the critical thinking skills required to recognize and handle them, we can help them make the most of the internet's vast resources without falling prey to its hidden dangers. These strategies are not just theoretical, they are actionable and effective in fostering a safe and positive online environment for children.

Let this guide serve as your personal compass and map to guide the young digital explorers in your life as they set sail on their digital adventures. It's not just about caution and awareness; it's about instilling confidence in both you and your child. Together, we can secure our children's online journeys, making them as enriching and trouble-free as possible.

Sean Atkinson, Chief Information Security Officer at the Center for Internet Security® (CIS®)

01

Dangers of sharing personal information online

Scenario

Emily, a curious 12-year-old, enjoys exploring social media and gaming forums. One day, she befriends Jake, a fellow gamer, in an online forum. They often discuss games, and Emily feels she's found a kindred spirit. Excitedly, she shares her gaming experiences, school stories, and favorite hangouts. Gradually, Jake inquiries about more personal details like her school's location and, eventually, her home address, promising to send her a game she's been longing for. Trusting and unaware of the risks, Emily shares her address.

Advice

- Never share personal details like your address or phone number with someone you meet online.
- Remember that people online might not be who they say they are.
- Tell a parent or trusted adult if someone asks for your personal information.

A week later, Emily's parents receive a suspicious package addressed to her. Concerned, they ask Emily about it, and she excitedly explains about her new online friend, Jake. Alarmed, her parents explain the dangers of sharing personal information online. Emily realizes her mistake and feels scared, realizing Jake might not be who he claimed to be.

Parental Advice

1. **Open Dialogue:** Regularly talk to your child about their online activities and friends.
2. **Educate on Risks:** Explain the dangers of sharing personal information online, including addresses, phone numbers, and school details.
3. **Supervise Online Interactions:** Monitor who your child interacts with online and discuss any new contacts.
4. **Privacy Settings:** Ensure social media and gaming profiles are private.
5. **Roleplay Scenarios:** Use hypothetical situations to teach your child how to respond to requests for personal information.
6. **Teach Critical Thinking:** Encourage your child to question online friends' intentions and verify their authenticity.
7. **Report Suspicious Behavior:** Instruct children to report any unusual or uncomfortable online interactions to you immediately.
8. **Regular Check-ins:** Check your child's devices and online accounts for unusual activity.
9. **Use Parental Controls:** Implement parental control software to monitor and restrict communications with unknown individuals.

02

Setting rules and boundaries around screen time and online usage

Scenario

Lucas, a 14-year-old high school student, has become increasingly absorbed in his smartphone, often spending hours on social media and video streaming sites. His parents notice his grades slipping, and he seems tired and irritable most mornings. Concerned, they realize they must set boundaries around his screen time, especially at night, to ensure he gets enough sleep and focuses on his studies.

Advice

- Balance your online activities with offline hobbies and interests.
- Respect the screen time rules set by your parents.
- Understand that these rules are for your well-being.

Lucas' parents sit him down for a discussion. He initially resists, arguing that all his friends are online late at night. However, his parents explain the importance of balance and the impact excessive screen time has on his health and academics.

Parental Advice

1. **Establish Clear Rules:** Define specific times for device usage, especially during evenings and study hours.
2. **Explain the Reasoning:** Help your child understand why these rules are in place, focusing on health and academic performance.
3. **Create Tech-Free Zones:** Designate areas like bedrooms and dining tables as device-free to encourage family interaction and better sleep hygiene.
4. **Lead by Example:** Model balanced screen time behavior yourself.
5. **Encourage Alternative Activities:** Promote hobbies and activities that don't involve screens.
6. **Use Technology Aids:** To enforce the rules, implement app blockers or screen time-monitoring apps.
7. **Regularly Review and Adjust Rules:** Be open to adjusting rules as your child grows and their responsibilities change.
8. **Reward Positive Behavior:** Acknowledge and reward adherence to screen time rules.
9. **Open Communication:** Maintain an open dialogue about how screen time affects daily life and responsibilities.
10. **Consistency Is Key:** Apply rules consistently and fairly, avoiding exceptions unless necessary.

03

Monitoring online activity and reviewing browser history

Scenario

A 10-year-old Sarah recently started exploring the internet more frequently for school projects and leisure. Her parents, Claire and David, want to ensure she accesses age-appropriate content. They decide to monitor her online activity regularly, including reviewing her browser history.

Advice

- Be mindful of the websites you visit and ensure they are appropriate.
- Know that your parents may check your browser history to keep you safe.
- If you stumble upon something inappropriate, inform your parents immediately.

One evening while checking Sarah's computer, Claire notices some search entries that lead to websites unsuitable for Sarah's age. Concerned, she and David realize they must talk with Sarah about internet safety and set up more stringent monitoring measures.

Parental Advice

1. **Open Discussion:** Start with a calm conversation about internet safety and the reason behind monitoring your child's online activity.
2. **Age-Appropriate Guidelines:** Set clear guidelines on what types of websites are appropriate for their age.
3. **Regular Checks:** Review browser history to understand your child's online interests and habits.
4. **Use Monitoring Tools:** Implement parental control software to filter content and monitor activity.
5. **Teach Responsible Usage:** Educate your child on the importance of responsible internet use and the potential risks of certain websites.
6. **Encourage Openness:** Foster an environment where your child feels comfortable discussing their online experiences.
7. **Use Browser Safety Features:** Use safe search settings on browsers and search engines.
8. **Create a Safe List:** Establish a list of approved websites for your child.
9. **Stay Informed:** Keep yourself updated about the latest online trends and potential associated risks.
10. **Parental Involvement:** Be involved in your child's online activities, suggesting websites and online resources they can use.

04

Enabling parental controls on devices and apps

Scenario

Jack and Amy, parents of nine-year-old Mia, are concerned about her exposure to inappropriate content on the internet. They decided to enable parental controls on her devices and apps to ensure she only accesses age-appropriate material. They notice Mia spends much time on her tablet, often downloading new apps without understanding their content.

Advice

- Understand that parental controls are there to protect you from harmful content.
- Ask for permission before downloading apps or making in-app purchases.
- Respect the boundaries set by these controls.

After setting up parental controls, Jack and Amy find Mia attempting to download a game unsuitable for her age. They realize this is an excellent opportunity to educate her about the importance of being cautious with app downloads and the content she consumes.

Parental Advice

1. **Choose Appropriate Controls:** Select parental tools that suit your family's needs and your child's age.
2. **Explain Their Purpose:** Discuss with your child why these controls are necessary and how they help protect them.
3. **Regularly Update Settings:** As your child grows, adjust the controls to reflect their maturity level.
4. **Monitor App Downloads:** Keep an eye on new apps downloaded and discuss each app's content.
5. **Encourage Informed Choices:** Teach your child to make informed decisions about what they download and view.
6. **Safe Browsing:** Ensure safe browsing settings are enabled on all devices.
7. **Involve Your Child:** Involve your child in setting up these controls, making it a learning process.
8. **Check Compliance:** Regularly ensure the parental controls are functioning as intended.
9. **Balance Trust and Safety:** While trusting your child is essential, ensuring their online safety is also crucial.
10. **Stay Informed:** Keep up to date with new parental control features and online safety trends.

05

Teaching children how to identify and avoid online scams and phishing attacks

Scenario

A savvy 13-year-old, Thomas often receives emails about his online gaming activities. One day, he gets an email claiming to be from a popular gaming platform, asking him to click on a link to claim a free game. Excited, Thomas clicks the link and unknowingly installs malware on his computer.

Advice

- Be skeptical of offers that seem too good to be true.
- Never click on suspicious links or download attachments from unknown emails.
- Inform a parent if you receive a strange message or email.

Thomas' parents notice the computer behaving strangely and discover the source. They realize Thomas needs guidance on identifying and avoiding online scams and phishing attacks.

Parental Advice

1. **Educate about Scams:** Teach your child about common online scams, including phishing emails and fraudulent websites.
2. **Show Examples:** Show examples of phishing emails and explain how to spot them.
3. **Never Click Suspicious Links:** Instruct your child never to click on links or download attachments from unknown sources.
4. **Verify Authenticity:** Teach your child to verify the authenticity of emails or messages by comparing them with official communication.
5. **Regular Updates and Security:** Ensure your computer has updated anti-virus software and discuss the importance of cybersecurity.
6. **Encourage Communication:** Encourage your child to consult you if they receive suspicious emails or offers.
7. **Personal Information Protection:** Reinforce the importance of not sharing personal information online.
8. **Critical Thinking:** Cultivate critical thinking in instances where your child receives offers that seem too good to be true.
9. **Safe Browsing Habits:** Teach and practice safe browsing habits.
10. **Report Suspicious Activity:** Instruct your child to report suspicious online activities.

06

Strong passwords and online security

Scenario

Max, a 15-year-old high school student, enjoys gaming and socializing online. He uses simple passwords for his online accounts for convenience. One day, he discovers his gaming account has been hacked and tampered with, causing distress and frustration.

Advice

- Use complex passwords with a mix of letters, numbers, and symbols.
- Never share your passwords with friends.
- Regularly change your passwords, especially for important accounts.

His parents, noticing his anxiety, learn about the incident and realize the importance of educating Max about solid password practices and online security.

Parental Advice

1. **Educate about Password Security:** Explain the importance of using strong, unique passwords for every account.
2. **Use Complex Passwords:** Encourage using a mix of upper- and lower-case letters, numbers, and symbols in passwords.
3. **Password Managers:** Introduce password managers to store and generate strong passwords securely.
4. **Regular Password Changes:** Advocate for changing passwords regularly and not reusing them across different platforms.
5. **Two-Factor Authentication:** Enable two-factor authentication (2FA) on accounts for added security.
6. **Discuss Online Risks:** Talk about the risks of weak passwords, such as hacking and identity theft.
7. **Practice Creating Passwords:** Have your child practice creating solid passwords and explain why each password element is important.
8. **Monitor Account Security:** Periodically check the security settings of your child's online accounts.
9. **Roleplay Scenarios:** Use scenarios to teach how to respond if they suspect their account has been compromised.
10. **Lead by Example:** Set a good example using solid passwords.

07

Avoiding inappropriate content online

Scenario

Sophie, a 12-year-old middle schooler, is curious and explores various websites. While searching for content for a school project, she accidentally stumbles upon a site with inappropriate material. Shocked and confused, she closes the site but remains disturbed by the experience.

Advice

- Stay away from websites that are not suitable for your age.
- Use search filters to help find age-appropriate content.
- If you see something disturbing, close it and tell an adult.

Her parents notice her discomfort and decide it's time to thoroughly discuss internet safety and how to avoid inappropriate content.

Parental Advice

1. **Open Communication:** Create an environment where your child feels comfortable discussing their online experiences.
2. **Use Content Filters:** Implement content filters and safe search settings on browsers and devices.
3. **Educate on Appropriate Content:** Clearly define what constitutes inappropriate content and why it's essential to avoid it.
4. **Monitor Internet Use:** Regularly check the websites your child visits and their apps.
5. **Discuss Accidental Exposure:** Talk about what to do if they encounter inappropriate content, which can include telling you immediately.
6. **Safe Browsing Habits:** Teach and encourage safe browsing habits.
7. **Age-Appropriate Websites:** Provide a list of age-appropriate websites and resources.
8. **Parental Controls:** Utilize parental controls to limit access to inappropriate material.
9. **Role Modeling:** Be a role model by demonstrating responsible online behavior.
10. **Stay Informed:** Keep up with the latest online trends and potential risks.

08

Cyberbullying and online harassment

Scenario

Ava, who is 13, becomes a target of cyberbullying by a group of students from her school. They post hurtful comments on her social media posts and send derogatory messages. Initially, Ava tries to ignore the bullying, but it starts affecting her self-esteem and mood.

Advice

- Be kind and respectful in all your online interactions.
- If you are being bullied online, save the evidence and tell an adult immediately.
- Stand against bullying and support friends who might be victims.

Ava's parents notice her withdrawn behavior and, upon inquiry, discover the ongoing cyberbullying. They realize they need to address this serious issue and ensure Ava's safety and well-being.

Parental Advice

1. **Listen and Support:** Listen to your child's experience without judgment and offer your full support.
2. **Document the Bullying:** Keep records of all bullying messages and posts.
3. **Report the Bullying:** Report the cyberbullying to the relevant social media platforms and, if necessary, to school authorities.
4. **Teach Online Etiquette:** Discuss the importance of kindness and respect online.
5. **Encourage Positive Interactions:** Encourage your child to engage in positive online communities and activities.
6. **Discuss Blocking and Reporting Tools:** Teach how to block and report users on social media platforms.
7. **Professional Help if Needed:** Seek professional help if bullying affects your child's mental health.
8. **Reinforce Self-Worth:** Build your child's self-esteem and resilience.
9. **Educate on Legal Consequences:** Discuss the legal implications of cyberbullying for both victims and perpetrators.
10. **Family Support System:** Create a family support system where your child feels safe and valued.

09

Speaking up about online harassment

Scenario

Liam, a 14-year-old gamer, frequently interacts with players online. Recently, he's received hostile and threatening messages from an anonymous player. Initially, he shrugs it off as part of the gaming culture, but he soon finds the messages increasingly disturbing.

Advice

- Never respond to threatening or uncomfortable messages.
- Tell a parent, sibling, teacher, or trusted adult if you feel harassed online.
- Block and report users who make you feel unsafe.

Hesitant to talk about it, Liam keeps the disturbing messages to himself until his older sister notices his anxiety and encourages him to open up. She then helps him talk to their parents about the situation.

Parental Advice

1. **Encourage Open Dialogue:** Foster an environment where your child can share their online experiences.
2. **Take Concerns Seriously:** Take your child's concerns about online harassment seriously.
3. **Understand the Situation:** Get a clear understanding of the harassment, including who is involved and what is being said.
4. **Report and Block the Harasser:** Guide your child in reporting and blocking the harasser on the platform.
5. **Review Online Safety Practices:** Discuss online safety and privacy practices.
6. **Emotional Support:** Provide emotional support and reassurance.
7. **Professional Counseling:** Consider professional counseling if the harassment has a significant emotional impact.
8. **Educate on Digital Footprint:** Teach about digital footprints and how online actions can have real-world consequences.
9. **Stay Informed about Online Platforms:** Be aware of the online platforms and communities your child is part of.
10. **Discuss Appropriate Responses:** Teach appropriate responses to online harassment, including not engaging with the harasser.

10

Monitoring social media and messaging apps

Scenario

Ella, a 16-year-old high school student, is active on multiple social media platforms. While respecting her privacy, her parents are concerned about her online interactions and the content to which she might be exposed.

Advice

- Think before you post. Would you be comfortable with everyone seeing it?
- Keep your profiles private and accept friend requests from only people you know.
- Discuss with your parents about what is appropriate to share online.

Ella's parents decide to talk with her about the importance of responsible social media use. They agree on a plan to periodically review her social media activity together, ensuring she is safe and responsible in her online presence.

Parental Advice

1. **Set Ground Rules:** Establish rules for social media use, including what's appropriate to post and share.
2. **Regular Check-Ins:** Have regular check-ins to review social media activity together.
3. **Respect Privacy:** Balance monitoring with respecting your child's privacy.
4. **Discuss Online Reputation:** Discuss how online behavior can impact your child's reputation and future opportunities.
5. **Educate on Privacy Settings:** Teach how to use privacy settings on different platforms.
6. **Encourage Positive Online Presence:** Encourage building a positive and respectful online presence.
7. **Address Risks of Oversharing:** Discuss the risks associated with oversharing personal information.
8. **Model Appropriate Behavior:** Lead by example in your own social media use.
9. **Stay Informed:** Keep up with social media platforms' latest trends and potential risks.
10. **Open Communication:** Maintain open lines of communication about your child's online interactions and experiences.

11

Consequences of posting inappropriate content online

Scenario

Ryan, 17, is a popular student, and he's active on social media. One evening at a party with friends, he posts several photos and videos on his social media accounts, some of which contain inappropriate content and language. The next day, he faces backlash from his school community and receives a warning from the school principal about his online conduct.

Advice

- Understand that what you post online can be seen by many, including future employers.
- Avoid sharing content that could embarrass you or others.
- Think about how your posts affect your personal image and reputation.

Ryan's parents learn about the inappropriate social media posts. They agree to sit down with Ryan and discuss how to post responsibly online.

Parental Advice

1. **Discuss the Impact:** Explain how online actions can have real-world consequences that affect reputation, relationships, and future opportunities.
2. **Role of Digital Footprint:** Teach about the concept of a digital footprint and how content, once posted, can remain online indefinitely.
3. **Encourage Responsible Posting:** Promote thinking twice before posting and considering the potential impact of each post.
4. **Review Privacy Settings:** Review privacy settings on social media platforms to control who can see posts.
5. **Case Studies:** Share real-life examples of how inappropriate content negatively affects others.
6. **Encourage Empathy:** Discuss the importance of empathy and respect for others online.
7. **Potential Legal Consequences:** Inform your child about the legal implications of posting harmful or offensive content.
8. **Build Awareness:** Keep your child updated about school policies and societal norms regarding online behavior.
9. **Monitor Social Media Use:** Regularly check your child's social media use while respecting their privacy.
10. **Promote Positive Online Presence:** Encourage building a positive and constructive online presence.

12

Critical thinking about online information

Scenario

Alice, a 13-year-old student, recently completed a school project based on information she found online. However, her teacher points out several inaccuracies in her work, citing unreliable sources.

Advice

- Not everything you read online is true. Learn to question and verify information.
- Cross-check facts using reliable sources.
- Discuss any confusing or controversial information you find online with an adult

Alice's parents, realizing she might not be discerning enough about the credibility of online information, decide to guide her in evaluating and verifying online content.

Parental Advice

1. **Teach Source Evaluation:** Show how to assess the credibility of a website or an online source.
2. **Discuss Fact-Checking:** Encourage double-checking facts with multiple reputable sources.
3. **Understand Bias:** Teach your child how to recognize bias and distinguish between opinion and fact.
4. **Encourage Questions:** Promote a questioning attitude towards information found online.
5. **Use of Reputable Sources:** Guide your child towards established, reputable news sources and educational sites.
6. **Real-Life Examples:** Use real-world examples to illustrate the consequences of misinformation.
7. **Critical Thinking Skills:** Foster essential thinking skills, including analysis and reasoning.
8. **Parental Involvement:** Be involved in your child's research projects and guide them in finding and evaluating sources.
9. **Digital Literacy Education:** Provide resources and tools for digital literacy.
10. **Safe Searching Techniques:** Teach effective and safe search techniques for research.

13

Reporting online threats or incidents

Scenario

Michael, a 15-year-old gamer, encounters a series of threatening messages from another player online. The messages escalate, leaving Michael feeling anxious and scared. He hesitates to tell his parents, worrying they might restrict his gaming.

Advice

- Do not engage with anyone who threatens or frightens you online.
- Save any threatening messages and show them to a trusted adult.
- Remember, it's not your fault if someone threatens you. Seek help.

When his parents notice changes in his behavior, they inquire and learn about the situation. They realize the importance of teaching Michael how to deal with online threats and the significance of reporting such incidents.

Parental Advice

1. **Create a Safe Environment:** Ensure your child feels safe and supported in discussing online experiences.
2. **Take Threats Seriously:** Acknowledge the seriousness of online threats and reassure your child of their safety.
3. **Document the Threats:** Instruct your child to save screenshots or records of the threatening messages.
4. **Report to Authorities:** Guide your child in reporting in-game threats to the game administrators and, if necessary, law enforcement.
5. **Review Online Safety Practices:** Discuss safe online practices, including privacy settings and choosing with whom to interact.
6. **Open Communication:** Maintain open dialogue about your child's online interactions.
7. **Monitor Online Activity:** Monitor your child's online activities while respecting their privacy.
8. **Teach Reporting Mechanisms:** Educate your child about the reporting features available on most gaming platforms.
9. **Professional Help if Needed:** Seek counseling if the incident impacts your child's mental health.
10. **Family Support:** Offer continuous support and understanding.

14

Risks of meeting strangers online

Scenario

Julia, 15, becomes friends with someone she met in an online chat room. After weeks of chatting, the person suggests they meet in person. Excited, Julia agrees and plans to meet them at a local café without informing her parents.

Advice

- Never agree to meet someone in person with whom you've talked only online.
- Tell your parents about any invitations to meet online friends.
- Remember, people online might not be who they claim to be.

Julia's older brother overhears her phone conversation and alerts their parents. Concerned, Julia's parents sit down with her to discuss the potential dangers of meeting someone online in person.

Parental Advice

1. **Discuss Online Stranger Danger:** Emphasize the risks of in-person meeting online acquaintances.
2. **Never Meet Alone:** Instruct never to meet an online friend alone or privately.
3. **Open Communication:** Encourage your child to discuss their online friends and plans.
4. **Educate on Safeguards:** Teach your child safety measures, such as meeting in public places and informing a trusted adult.
5. **Roleplay Scenarios:** Use roleplaying to practice handling invitations to meet.
6. **Monitor Online Interactions:** Keep an eye on your child's online interactions while respecting their privacy.
7. **Build Trust:** Build a trusting relationship where your child feels comfortable discussing online activities.
8. **Understand Their Perspective:** Listen to your child's reasons for wanting to meet online friends and address any misconceptions.
9. **Set Boundaries:** Establish clear rules about online relationships and in-person meetings.
10. **Parental Supervision:** Offer to accompany your child if a meeting with an online friend is ever considered.

15

Rules around online gaming and chat rooms

Scenario

Alex, 10, spends a lot of time playing online games with chat features. His parents notice him becoming increasingly agitated after gaming sessions and overhear him using inappropriate language during in-game chats.

Advice

- Be respectful to others when playing games or chatting online.
- Do not share personal information with players you meet online.
- If someone makes you uncomfortable, stop chatting and tell an adult.

Alex's parents set rules around his online gaming and chat room usage to ensure a healthier gaming environment.

Parental Advice

1. **Set Time Limits:** Establish specific times for gaming to prevent excessive play.
2. **Monitor Chat Rooms:** Keep an eye on your child's language and behavior in chat rooms.
3. **Discuss Appropriate Behavior:** Talk about respectful communication and behavior online.
4. **Game Selection:** Choose games appropriate for your child's age and maturity level.
5. **Encourage Breaks:** Promote taking breaks to reduce screen time and stress.
6. **Teach Online Etiquette:** Educate your child on digital etiquette and the impact of words.
7. **Parental Controls:** Use parental controls to restrict access to specific chat features.
8. **Balanced Activities:** Encourage a balance of online and offline activities.
9. **Open Dialogue:** Maintain open communication about your child's experiences and feelings around gaming.
10. **Lead by Example:** Model appropriate online behavior yourself.

16

Privacy settings on social media and messaging apps

Scenario

Natalie, a 16-year-old high schooler, enjoys connecting with friends and sharing her life on social media. She often posts pictures of her daily activities, unaware of her profile's public visibility. One day, she receives messages from unknown people commenting on her posts, making her uncomfortable.

Advice

- Keep your social media profiles private and only share with people you know.
- Think before you post. Once something is online, it can be hard to remove.
- Regularly review your privacy settings with a parent.

Her parents, noticing her distress, check her social media accounts and realize that her posts are visible to anyone online. They decide it is crucial to educate Natalie on the importance of privacy settings and managing her online presence more securely.

Parental Advice

1. **Review Privacy Settings Together:** Go through the privacy settings on each social media platform with your child, ensuring their profiles are set to private.
2. **Educate on Information Sharing:** Discuss what kind of information should not be shared publicly, such as location, contact information, and personal plans.
3. **Encourage Regular Updates:** Remind your child to check and update their privacy settings regularly.
4. **Discuss the Risks of Oversharing:** Discuss the potential risks of oversharing personal information, including unwanted attention and data privacy concerns.
5. **Teach Digital Footprint Awareness:** Explain how online behavior can impact your child's reputation and future opportunities.
6. **Model Appropriate Behavior:** Demonstrate responsible social media usage yourself.
7. **Monitor Social Media Use:** Monitor your child's social media activity, ensuring it aligns with the family's online safety guidelines.
8. **Promote Positive Online Presence:** Encourage your child to use social media positively and creatively.
9. **Create a Safe Environment:** Foster a family environment where your child feels comfortable discussing online issues or concerns.
10. **Stay Informed:** Keep up with the latest social media trends and privacy tools to guide your child effectively.

17

Being respectful and kind online

Scenario

Jason, 15, actively participates in various online and social media forums. One day, his parents overhear him speaking disrespectfully to another player in an online game.

Advice

- Treat others online as you would like to be treated.
- Avoid saying hurtful or mean things on the internet.
- Remember, there's a real person on the other side of the screen.

Concerned about this behavior, Jason's parents decide to address the importance of being respectful and kind in all online interactions, emphasizing that the anonymity of the internet does not excuse poor behavior

Parental Advice

1. **Discuss Online Etiquette:** Talk about treating others respectfully, even online.
2. **Set Expectations:** Clearly outline acceptable and respectful behavior online.
3. **Lead by Example:** Model positive and respectful online interactions yourself.
4. **Consequences for Misbehavior:** Establish consequences for disrespectful or unkind behavior online.
5. **Empathy Training:** Encourage empathy by asking your child how they would feel if someone spoke to them similarly.
6. **Monitor Online Interactions:** Periodically check your child's online communications, ensuring they align with the family's values.
7. **Encourage Positive Communities:** Guide your child to online communities promoting positivity and respect.
8. **Discuss the Impact of Words:** Talk about how words can affect others, even when communicated digitally.
9. **Promote Self-Reflection:** Encourage your child to reflect on their online behavior and its impact on others.
10. **Teach Conflict Resolution:** Offer strategies for handling disagreements online in a respectful manner.

18

Monitoring online purchases and subscriptions

Scenario

Lily, 14, can access a family tablet with a linked credit card for app purchases. Her parents, Lisa and John, trust her judgment but notice charges for several online subscriptions and games of which they disapprove.

Advice

- Ask for permission before buying anything online.
- Be aware of in-app purchases and subscriptions.
- Understand the value of money and spend wisely.

Realizing the need for more precise guidelines and monitoring, Lisa and John sit down with Lily to discuss responsible online spending and the importance of seeking purchase permission.

Parental Advice

1. **Set Spending Limits:** Establish clear rules on the amount your child can spend and what types of purchases are allowed.
2. **Require Permission for Purchases:** Insist that your child asks for permission before purchasing or subscribing.
3. **Review Purchases Together:** Regularly check the purchase history with your child to understand their spending habits.
4. **Educate about Online Scams:** Warn your child about scams and the importance of verifying the legitimacy of websites and apps before purchasing.
5. **Link to a Limited Account:** Consider linking the tablet to an account with limited funds to control spending.
6. **Discuss the Value of Money:** Discuss the value of money and budgeting.
7. **Promote Earned Rewards:** Implement a system where your child can earn credits or allowances for purchases through chores or good behavior.
8. **Use Parental Controls:** Utilize parental control features to approve or decline purchase requests.
9. **Encourage Research before Buying:** Teach your child to research and read reviews before purchasing online.
10. **Model Financial Responsibility:** Demonstrate responsible financial behavior in your online purchases.

19

Recognizing and avoiding online predators

Scenario

Kevin, 12, often chats with friends and joins various online groups related to his hobbies. One chat group member starts showing particular interest in Kevin, asking personal questions and suggesting a private meet-up. Kevin feels uneasy but isn't sure how to handle the situation.

Advice

- Be cautious about sharing personal information online.
- If an online friend wants to meet in person or asks uncomfortable questions, tell an adult.
- Trust your instincts. If something feels wrong, it probably is.

Kevin's older sister notices his discomfort and informs their parents. Realizing the potential danger, they talk to Kevin about recognizing and avoiding online predators.

Parental Advice

1. **Educate about Online Predators:** Explain what online predators are and their tactics to groom and manipulate children.
2. **Recognize Warning Signs:** Teach your child the warning signs, such as someone asking for personal information, sending gifts, or suggesting secrecy.
3. **Never Share Personal Information:** Reinforce the rule of never sharing personal details, photos, or in-person meetings with online acquaintances.
4. **Encourage Open Communication:** Create a safe space for your child to discuss any uncomfortable online interactions.
5. **Review and Monitor Online Activities:** Review your child's online activities and the people with whom they interact.
6. **Teach to Trust Instincts:** Encourage your child to trust their instincts and report anything that makes them uncomfortable.
7. **Safe Internet Use Practices:** Reinforce safe internet practices, including privacy settings and browsing.
8. **Roleplay Scenarios:** Use roleplaying to practice responding to suspicious online behavior.
9. **Report Suspicious Behavior:** Instruct your child to report suspicious behavior on platforms and to adults.
10. **Professional Advice if Needed:** Seek professional guidance if you suspect an online predator is targeting your child.

20

Digital citizenship and responsible online behavior

Scenario

Megan, a 13-year-old, avidly uses social media and online platforms. Her parents, Mark and Sarah, notice that while Megan is technologically savvy, she is not fully aware of digital citizenship responsibilities.

Advice

- Your actions online affect others. Be a good digital citizen.
- Respect other people's privacy and opinions online.
- Understand the long-term effects of your online behavior.

Mark and Sarah observe Megan occasionally sharing her friends' posts without their permission and engaging in heated debates online. Concerned, they decide it is time to teach Megan about digital citizenship and responsible online behavior.

Parental Advice

1. **Define Digital Citizenship:** Explain the concept of digital citizenship and its importance in today's digital world.
2. **Discuss Online Responsibilities:** Talk about the responsibilities of using the internet, including respecting others' privacy and opinions.
3. **Encourage Respectful Communication:** Teach your child to communicate respectfully and constructively online, even in disagreements.
4. **Educate on Privacy and Security:** Discuss the importance of online privacy and security.
5. **Model Positive Behavior:** Demonstrate positive and responsible digital behavior.
6. **Teach About Consent:** Emphasize the need to get consent before sharing others' content.
7. **Impact of Online Actions:** Discuss how online actions can have real-life consequences.
8. **Balance Online and Offline Life:** Encourage a healthy balance between online activities and offline relationships and activities.
9. **Critical Thinking:** Foster essential thinking about the content your child consumes and shares.
10. **Open Dialogue:** Maintain an open and ongoing dialogue about your child's experiences and learnings in the digital world.

Conclusion

Emma

Being a kid in today's online world is exciting but sometimes scary. This guide helped me see that my parents aren't just being strict or nosy when they ask about what I'm doing online. They're trying to keep me safe from stuff that I didn't even know could be dangerous. I learned a lot about scams and how people might not always be who they say they are on the internet. Now, I feel more confident about using the internet, and talking to my parents about it doesn't feel like such a big deal anymore. Knowing how to protect myself and still have fun online is cool!

Sean

As a parent, navigating the complexities of the digital world alongside my child has been both challenging and enlightening. Throughout this journey, I've learned that my role isn't just to monitor and mentor. We've built more trust and understanding by engaging actively with my child's online activities, discussing the scenarios explored in this guide, and setting boundaries. I've seen firsthand how empowering it is for a child to know the dangers and the vast potential of the internet. This guide has equipped me with the tools to guide and support my child, making our digital experiences positive and productive. I hope other parents find this guide as invaluable as I have in fostering an environment where our children can safely learn, create, and connect.

About the Authors

Emma Atkinson

Emma Atkinson is a freshman attending Emma Willard School in Troy, NY. Her favorite subjects are English Literature and Latin. In her free time, she enjoys playing softball and ice hockey.

Sean Atkinson

CIS Chief Information Security Officer

Sean Atkinson is Chief Information Security Officer of CIS. He uses his broad cybersecurity expertise to direct strategy, operations, and policy to protect CIS's enterprise of information assets. His job responsibilities include risk management, communications, applications, and infrastructure.

Prior to CIS, he served as the Global Information Security Compliance Officer for GLOBALFOUNDRIES, serving Governance, Risk and Compliance (GRC) across the globe. Prior to GLOBALFOUNDRIES, Atkinson led the security implementation for the New York State Statewide Financial System (SFS) implementation from 2007 to 2014, and his last role and responsibility was as the Internal Control, Risk and Information Security Manager.

Atkinson was born in Brooklyn, New York, and lived in England for 18 years, graduating from Sheffield Hallam University in 2000. After moving back to the United States, he has pursued multiple degrees and certifications in the IT arena.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
CenterforIntSec
@CISecurity
TheCISecurity
cisecurity