TOPICAL PAPER
www.centerontransition.org
Center on transition innovations VCU

Promoting Internet Safety Among Autistic Users

Staci Carr
VCU Center on Transition Innovations
April 2023

Introduction

The online world is a vast resource of information that can help you learn, be a social outlet, and offer entertainment. But it also has the potential threats of cyberbullying, catfishing, identity theft, and fraud–to name a few. With approximately 95% of teenagers (12-17 years) being online, it is best to know how to be safe on the internet (Joshi, et al., 2019).

This is of particular importance to autistic learners. The internet offers a space that reduces the need for in-person communication and social interaction. This may make it more appealing to autistic users. Developing online friendships can be both rewarding and less stressful. That said, ensuring online safety is of utmost importance. The following tips will help you increase internet safety.

Cyberbullying

Cyberbullying occurs through electronic communication such as text messages, email, social media sites, blogs, forums, or even games with chats. This type of bullying has become more prevalent over time. One study described that 42.8% of teens (12-18 years) have reported experiencing at least one form of cyberbullying (Gohal, et al., 2023). Cyberstalking, a form of cyberbullying, happens when someone will not stop reaching out to a person on social media or other technology even after being asked to stop.

What Can I Do?

- Make sure that only people an individual knows and trusts can see their social media profile.
- Teach how to “unfriend” and block people who are abusive online.

- If cyberbullying happens, collect data (e.g., screenshots of texts, online messages, email, etc.). This information will help you inform school administrators or the police.
- Report cyberbullying to school authorities and the content provider (e.g., Facebook, YouTube, etc.).
- Ask questions and provide space for conversation about cyberbullying.
- If there is a threat of physical harm, call the local police.

Internet Scams

Cybercriminals and scammers are on the rise and so is their creativity when it comes to scamming. Because autistic individuals may lack the awareness of what a scam is (e.g., "too good to be true") they may fall victim to a scam. Scammers may make promises to you that result in you losing money. They may offer a loan, a prize like a foreign lottery, a government grant, an inheritance, an opportunity to work from home, or more. The catch is, they want payment upfront before you can receive your benefit. There are different types of scams.

Phishing: When you receive an unsolicited message asking to provide sensitive data like passwords, credit card numbers, bank account details, social security numbers, etc.

Identity theft: When your identity is stolen and used to commit fraudulent acts against you like making purchases with your credit card information.

Social engineering: When someone pretends to be another person and tries to gain access to your computer or phone. For example, a person pretending to be your friend asks for personal information.

Spoofing emails: You receive emails that look like they are from a legitimate source but they are actually from someone else.

What Can I Do?

- Review the types of internet scams that are out there. Stay up to date with current scams.
- Report the scam to the Federal Trade Commission so they can help protect others. Report the scam to the FTC online, or by phone at 1-877-382-4357 (9:00 AM - 8:00 PM, ET).

Inappropriate Content

As mentioned above, the internet is an expansive space with all sorts of information. Some of this content can be harmful or disturbing, which can lead to a variety of issues including trauma. Exposure to violent images, pornography, hate speech, and abuse can cause significant distress.

This can happen through random searching, so it is essential to stay alert. Accessing things like child pornography, even by accident, can have tremendous legal consequences.

What Can I Do?

- Use Google's SafeSearch when browsing the internet. It is not 100% accurate, but it allows you to filter out things like pornography and explicit images when you are googling on your phone, tablet, or computer.
- Use a web filter to track websites accessed to block inappropriate content. These filters can manage screen time, restrict which websites your kids can visit, keep up with kids with location alerts and check-ins, and track texts, email, YouTube, and 30+ apps and platforms. You can also get alerts for cyberbullying, online predators, suicidal thoughts, and more.
- Install anti-virus and anti-malware protection to keep your computer safe from viruses, as well as to keep an individual from seeing inappropriate pop-ups. Make sure that the software is up to date.

Sharing Personal Information

Knowing when and how much personal information to share can be challenging and confusing. Personal information includes things like your address, phone number, financial situation or bank account information, social security number, health status, or any of this information about your family. When you share personal information online, it can be dangerous if it gets into the hands of hackers or scammers.

What Can I Do?

- Never give out personal information by text, email, dating sites, or through social media!
- You CAN give personal information if it is appropriate to do so.

What You Can Share and To Whom

Email address: Share it with someone you just met and want to get to know better, if you are on a secure account website, and if you are applying for a job, mentorship, or volunteer work.

Phone number: Share it with someone you already know, law enforcement, applications, someone you want to get to know better, and on health forms.

Address: Share with people you already know and TRUST, transportation companies (Lyft, Uber, Care Van), on applications, and health forms.

Debit card: Make online purchases on secure websites only! NEVER SHARE YOUR PIN!

Bank account information: Share with the teller at a bank, a parent or guardian as needed, to set up automatic payments for bills, and employers for direct deposit.

Social media profile: Share with friends or family that you want to keep in touch with and people you met and would like to connect with in the future.

Conclusion

Keeping safe while on the internet can be challenging, but it is very important. Make sure that your computer has software to help protect against viruses and inappropriate content. Creating tighter online security measures and staying vigilant will help support a safe online environment for you and your family.

References

Gohal, G., Alqassim, A., Eltyeb, E. et al. (2023). Prevalence and related risks of cyberbullying and its effects on adolescent. *BMC Psychiatry 23*, 39. https://doi.org/10.1186/s12888-023-04542-0

Joshi, S.V., Stubbe, D., Li, S. T., & Hilty, D.M. (2019). The use of technology by youth: Implications for psychiatric educators. *Academic Psychiatry, 43*, 101-109.

The contents were developed under a contract (#881-APE62524-H027A220107) from the Virginia Department of Education. Virginia Commonwealth University, including the School of Education and Department of Physical Medicine and Rehabilitation, is an equal opportunity/affirmative action university providing access to education and employment without regard to age, race, color, national origin, gender, religion, sexual orientation, veteran's status, political affiliation or disability. If special accommodations are needed, please contact the Center on Transition Innovations at transition@vcu.edu.

VIRGINIA DEPARTMENT OF EDUCATION