A Helpful Online Safety Guide for People With Autism Spectrum Disorders

Last Updated by [Gray Williams](#) on June 17, 2019

People from all walks of life and all kinds of backgrounds fall victim to online bullying and cybercrime, but studies have shown that those with an **autism spectrum disorder (ASD)** are **more susceptible to online threats** than others.

ASD is a developmental disorder that affects behavior and communication. People on the Autism Spectrum tend to live a relatively normal life but can need supervision and lack judgement – a trait that has been identified as dangerous when left to their own devices in cyberspace.

Not only are ASD children and adults at risk from others, but they can also develop compulsive online habits and internet addictions, and can be more deeply affected by exposure to inappropriate content.

Everyone should feel safe online. It's therefore extremely important to make sure you have adequate online security and remain internet vigilant.

To help you surf with ease and reduce your vulnerability to attack, take a look at our **Internet Safety Guide for people with ASD**. ([Share on Facebook](#))

Table of Content:

Common Online Issues

There are always an array of threats surfing along the waves of cyberspace. Familiarize yourself with what they are and be extra vigilant – a plan of action is most definitely in order. Below, we have selected the most common online issues faced by those with ASD and provide tips on how to take control of the situation.

1. Cyberbullying

Cyberbullying has become a more common trend across the internet, especially affecting children and those with ASD. The bullies use digital platforms, like social media or internet chat forums, to harass and intimidate their victims. Sometimes, this harassment can escalate into real-world threats and bullying. Anyone can become the target of a cyberbully, despite their age, background or lifestyle.

According to the Journal of Mental Health Research in Intellectual Disabilities, those with intellectual and developmental disabilities are more likely to become the victim of cyberbullying. The anti-bullying alliance has also found that those with disabilities are more susceptible to cyberbullies.

More is being done to understand the phenomena and help build a safer environment online. However, cyberbullying can sometimes be difficult to recognize.

Text-based communication sometimes struggles to convey the same level of meaning and context as face-to-face conversations. Because of this, it can sometimes be hard to tell if someone is intentionally trying to bully, or if it's a misunderstanding. But, if a person sends you abusive messages, or tries to intimidate or embarrass you online, this is most definitely cyberbullying.

The Long-Term Effects of Cyberbullying

Bullying can damage your self-worth and/or affect your mental health. Ongoing harassment could lead you to withdrawing from society, making it difficult for you to interact with friends and family. If left unaddressed, the impact of cyberbullying can run deep, and for a long time.

Even though this sounds scary, don't let it deter you from exploring online and forming meaningful friendships with people over the internet.

Different Types of Cyberbullying

Cyberbullying is a beast with many faces, the most common of which is abusive messages received through email, text message, and instant chat. However, it's not only through these means that online bullies can get to you.

Cyberbullying might also manifest itself in the following guises:

- A person spreading gossip and rumors about you online, to your friends or even strangers.
- Someone who posts statuses and comments intending to humiliate you, or altering the way in which other people perceive you.
- Threats being made to you through social media and other avenues of online communication.
- Someone who uses their online profiles to share information, videos, or photos of you without your consent, or after you have asked them to stop.
- A person who uses your online profiles and information to stalk you online and/or in real life.
- Someone who hacks into your online accounts or impersonates you with the intention of using your name and reputation to spread inappropriate or harmful content. This is most commonly known as fraping.

How to Prevent Being Bullied Online

Recent research suggests that cyberbullying tends to occur when certain risk factors aren't mitigated. Although cyberbullying is hard to stop, you can take steps to prevent yourself from becoming a victim.

The **first step is to change the settings** on your social media accounts so that **your profiles can only be seen by people you know and trust**. Cyberbullies are opportunistic by nature, so you're at greater risk of experiencing online harassment if strangers can easily contact you.

Similarly, you should always avoid opening messages or accepting friend requests from people who you don't know. The ability to hide behind a computer screen while attacking someone often removes a cyberbully from the real-world

consequences of their actions, and so they often pick on someone who isn't in their social circle or someone they don't know.

6 Tips to Avoid Cyberbullying

- **Secure your social media accounts.** Set your security levels to 'friends only' so that strangers can't see your profile or send you messages.
- **Don't post personal information online.** Never post information such as your location, address, phone number, school, or workplace online. This will help to prevent cyberstalking, and also means bullies won't be able to contact you face-to-face or on the phone.
- **If someone sends you abusive messages, don't take the bait.** Most bullies' primary goal is to elicit a reaction from their target. If you respond, it might encourage them to continue, so it's best to refrain from giving them what they're looking for. Most bullies will simply give up and leave you alone if you don't reply.
- **Report them.** If someone is bullying your or someone you know, report their post to the platform's support team. A member of staff will review the content and make a decision to either delete it or allow it to remain. In more serious cases, they may even take action against the bully by blocking or banning them.
- **Block the bully.** Blocking someone will prevent them from accessing your profile and contacting you in the future.
- **Talk about it.** Let a trusted friend or family member know what's going on. They might be able to help you or give you some handy advice.

2 Understanding the Context of Online Messages

Online Misunderstandings

It is possible to misunderstand a situation when communicating with someone over the internet. It's easy to miss the context or meaning of someone's comment in the absence of social cues, and this can cause online discourse to go off-track, or even turn into a heated argument.

Here are the best practices for avoiding misunderstandings online:

- Keep in mind that not everything you read online is true and not everyone with whom you speak will be honest.
- If something is unclear, ask the person to clarify what they mean before sharing your opinion.
- Use reliable sources to double check facts and information so you don't take on or share something that is inaccurate.
- Remember to be polite and calm even when you are sure that somebody is wrong or if you feel they are being rude.
- Look out for admins and moderators in groups and forums to mediate online discussions if they become uncomfortable or argumentative.
    Online forums, like [Talk About Autism](#), are built specifically for people with ASD to socialize and make friends. Most of these forums have moderators who monitor the discussions and are trained to offer mediation if they spot a misunderstanding.

12 Ways to Improve Social Media and Online Communication

There are a lot of benefits for using social media, especially for people on the Autism spectrum who may have trouble interacting with people. However, there are some drawbacks to putting all of your information on social networks. Here are 12 tips that can improve online communication and minimize the risk of being misunderstood.

1. **Never add your boss, teacher, or supervisor on social media.** If you're friends online, they'll be able to see the content on your profile, which may lead to misinterpretations over your character. If their opinion of you is altered by what they see, it could hinder your ability to get a promotion.
2. **Never comment about your workplace online** especially if you're complaining about your job. It might seem innocent to you, but it could cost your job if it gets back to your bosses or colleagues. Additionally, most workplaces now have rules against posting about your work on social media.
3. **Refrain from posting content that might skew other people's opinion of you**, such as angry rants. Potential employers will usually look you up online and they may base their opinion on you from what they see, even if it doesn't actually represent who you are.
4. **Always meet a new online friend during the day and in a public place.** Always tell someone where you are going, who you are meeting and any change of location. To be extra careful, you could take a trusted friend or family member with you. Don't go anywhere secluded or follow them back to their house. If something feels 'off,' leave.
5. **Keep your passwords safe and don't hack into other people's accounts or websites**, even if you can. People with ASD often find themselves the victim of a manipulative person who will ask them to break the law or hack a computer, but it's illegal to do so.

6. **Don't believe everything that you read online – particularly on social media**. A lot of users spread misinformation over the internet and even exaggerate their lives to look good.
7. **Don't compare your life with someone else's on social media** – you're only seeing the highlights of their life, not the regular everyday experiences.
8. **Always be polite in your online discourse and avoid arguments**, even when you feel that the other person is wrong.
9. Remember that most **internet users regard typing in capitals as the digital equivalent of yelling**, and in this context, it can be viewed as rude to type in ALLCAPS.
10. You can **use emojis or emoticons to better express the context and meaning of your words**. For example, adding a smiley face to the end of a sentence will show that you are happy, or being friendly.
11. **If someone is making you feel uncomfortable or unsafe, leave the situation** and block them.
12. **Never send explicit photographs of yourself or forward on pictures of anyone else**. If you share photos without consent, or photos of a minor, you are breaking the law and may face legal consequences.

3 Becoming a Victim of a Scam, Manipulation or Hacking

Scammers and hackers are unfortunately a part of everyday online life. To put it simply, some people have ill intentions and wish to manipulate others for their own gain.

They will present themselves as someone who wants to become your friend, or even a potential romantic partner. They will work hard to build a relationship to gain your trust, then rip you off!

Scammers, hackers and cybercriminals will do this for a variety of reasons. For example, they may try to con you into sending them money or committing a crime on their behalf.

They may also be phishing for your personal information – like your passport details – to steal your identity or pose as you online.

Best Practices for Avoiding Scams and Manipulation

- Don't give anyone personal information, such as your address, phone number, or ID number.
- Never divulge your banking or credit card information online – remember that some scammers may contact you pretending to be your bank. Your bank will never contact you asking for personal and private information.
- Don't tell anyone where you or your friends and family work or go to school.
- Consider using a pseudonym instead of your real name – lots of people use their first and middle names, or create an entirely new name for themselves.
- Be careful when agreeing to meet up with people you've met online.
- Don't send money to anybody you meet online – if somebody asks you to send them cash, it's likely they are trying to scam you.
- Never click any links to websites that you don't recognize as they may take you to a website that will compromise your computer's security.

> If you think that you may have been the victim of a scam, it is important that you contact your bank and local law enforcement agency immediately.

Play it Safe

The **Center on Secondary Education for Students with Autism Spectrum Disorder** have created a **memorable acronym for staying safe online**, Play it Safe.

Personal information – never share your personal information online.

Let a friend or family member know if someone has asked you for this information, or if you don't feel safe.

Attachments – remember that email attachments might contain malware that can damage your computer and harvest your private information. Don't open them unless it's a file that you have been expecting from someone that you trust.

Your feelings are important. If something makes you feel uncomfortable or unsafe, stop and let somebody know.

Information – remember that not everything you read online is true.

Take breaks from your computer often to socialize, stretch, and give your eyes a rest.

Spend your money safely. Don't buy things from unfamiliar stores or links, and don't send people money.

Act politely and don't say things online that you wouldn't say in real life.

Friends online should stay online – if someone asks to meet up, tell them no.

Enjoy yourself and have fun!

4 Exposure to Inappropriate Content

For as many wonderful and informative pieces of information you find online, there are equal amounts of inappropriate and harmful content hidden away. Sometimes, you might stumble across depictions of violence, pornography, and illegal content that most people would prefer to avoid. Accessing things like child pornography, even by accident, can have disastrous legal consequences, so it's important to safeguard yourself against this.

Tools to Block Inappropriate Content

1. SafeSearch:

Google's SafeSearch blocks explicit content from your Google search results. Although it isn't always 100% accurate, it allows you to filter out things like pornography and explicit images when you're googling on your tablet, phone, or computer.

How to set up SafeSearch:

Go to 'settings' button on your Google homepage, then navigate to search settings. Under SafeSearch filters, select the box next to the 'turn on SafeSearch' option, and be sure to click save before you navigate away.

You can check out Google's SafeSearch guide to learn how to [enable it on your Android or iOS device](#).

2. Internet filters:

Web filters, like Net Nanny, monitor the websites you access in order to block inappropriate content. You can customize the things your filter looks for, and even whitelist websites you deem as safe. This is a great tool for adults who want to filter out content that's not safe for work as well as parents looking to keep their kids safe online.

3. Advert and pop up blockers:

We've all heard stories of friends who've had people walk up behind them when they're using their computer, only for an unexpected explicit pop-up to come on the screen at that very moment. You can protect yourself from these potentially disastrous incidences by installing a pop-up and ad blocker on your browser.

4. Anti-virus and anti-malware protection:

Some viruses and malware will cause explicit pop ups to grace your screen at inopportune moments. A good, up-to-date anti-virus will not only protect your computer from damaging infections, but it will also keep you shielded from inappropriate content.

5. Links:

Avoid clicking on links you don't recognize. Even if the message is sent to you by a friend, don't click on a link you don't recognize, or you aren't expecting. You will often receive spam messages via text messages and email that ask you to click on a link to access their website or even a prize, but doing so will leave you at risk of a virus or scam.

5 Sensory Overload on the Internet

For those of us who experience sensory sensitivity, electronic devices and the internet can trigger an all-round overload. Loud noises, bright backlights, unexpected music, and auto-playing videos are just a handful of the irritants that can overwhelm.

Thankfully, there are steps you can take to minimize the sensory impact.

- Adjust your screen's brightness levels and invest in an app that blocks blue light on your device. Although it will make your screen appear with a slightly orange tint, blocking out blue light is a must for decreasing the strain that backlights put on our senses. Apps to block blue light are available on most devices, and they'll even help you get to sleep faster and minimize the impact of light-sensitive migraines.
- Switch video and audio autoplay off on your social media platforms.
- Invest in a 'quiet' keyboard and mouse to reduce the clicking noises as you type.
- White noise is a great tool to soothe the senses. It can also drown out irritating sounds, like the hum of your computer, or your noisy neighbors! White noise videos are available for free on YouTube, or, alternatively, you can purchase a white noise machine.

6 Internet Addiction

The allure and ease of socializing online can negatively impact your drive to socialize in the real world. Online addiction is a serious issue and iT affects many people. Studies suggest that people who are prone to obsessive behaviors are at greater risk of developing an internet addiction. People with ASD and anxiety disorders are at particularly high risk.

It's easy to see why – the internet offers sanctuary and an easy way to connect and communicate with peers. When most of your friends are internet-based, that's where you will want to spend most of your time.

> It's **crucial for your mental and physical health to develop and maintain relationships in the real world**. The internet is a wonderful tool, but if it interferes with your ability to spend time with friends and family, it might be time to take a break.

Tips to Counter Internet Addiction

- Set yourself a time limit when you're on the computer. You might like to set a timer for an hour or two and log out when the time is up.
- Create a roster or make plans to spend a certain amount of time with friends and family, or enjoying hobbies and exercise, each day. Include your online time in your roster, but plan other activities for your free time as well.
- Make sure you have completed all the other tasks you need to do, like chores, before you go online each day.
- Use specially designed apps to remind you to take a break. Programs like Offtime monitor your usage and show you how much time you've been spending on social media. You can even set them to block certain sites, like Facebook, during certain times of the day.
- Set your social media push notifications to silent on your phone or tablet. This way, you'll receive them when you login and not when you're busy with other activities. If you feel that you might be falling victim to an internet addiction, you can ask your doctor for a referral to an experienced therapist who will be able to give you more advice.

7How to Protect Yourself on Popular Social Networks

Below, we have compiled a short guide to keeping yourself safe on some of the most popular social media networks. We delve into their risks, and how to change your account settings to avoid explicit content, scammers, fake profiles, and cyberbullies.

Facebook

What are some of the main risks on Facebook?

- it is easy for scammers to befriend and trick you by using fake profiles.
- There is a medium to high risk of being exposed to links that will take you to scam websites that phish for your personal information.
- Cyberbullies often use Facebook to harass their victims.
- Although it is against Facebook's policies, you may be exposed to explicit posts that their content filters haven't detected.
- Features like video autoplay can trigger sensory overload.
- Social media, as a whole, can be addictive.

Ways to protect yourself on Facebook

- **Leave out personal information:**
  Although Facebook asks for your first and last name, avoid giving it if you can. Instead, many people use a pseudonym or create a fake last name. This will make it difficult for people to track you down on other platforms or in real life.

  Avoid customizing your 'about me' section too much. You should never tell Facebook where you live, work or study.

  If you're using a device with GPS, don't allow Facebook to post your location. The easiest way to do this is to block Facebook from accessing your device's location information. You can usually find this setting on your device under Settings > Privacy > Location Services.

- **Make your account private:**
  Make sure that your profile is private so that only your friends can see your statuses and send you messages. This reduces your risk of encountering cyberbullying by putting you in charge of who can contact you. Keep in mind that strangers will still be able to read any comments you make on your friends' posts and on public pages.

- **How to set your posts to friends only:**
  Once you've opened the status dialog box, click the privacy setting drop-down menu in the lower bar. It will say either 'friends' or 'public.' If it says 'friends,' that means only the friends you have accepted will see this post. If it's set to 'public' click on it and select 'friends' before you hit the post button.

- **How to set your profile to private:**
  Login to Facebook and select the arrow at the top of your page in the home bar. From here, select 'settings'.

  When your settings page loads, select 'privacy' in the sidebar. This will load two categories of privacy settings for you to alter.

  There are two privacy options under 'your activity'. For the best privacy possible, set them as follows:

- **Who can see your future posts?**
  This should be set to 'friends only,' so that strangers can't see your private status updates.

- **Limit the audience for posts you've shared with friends of friends or public?**
  If you opt to change this to 'friends only', it will increase the privacy of all your past posts so that strangers can no longer view them.

  Next, decide how people can find and contact you.

- **Who can send you friend requests?**
  If you're not interested in receiving friend requests from strangers, set this option to friends of friends. Unfortunately, there is no way to completely eliminate people sending you requests, but this will reduce the occurrence by quite a bit.

- **Who can see your friends list?**
  For optimal security, set this one to 'friends' or 'only me'.

- **Who can look you up using the email address/phone number you provided?**
  If you're worried about strangers or bullies tracking you down using your email address or phone number, set this one to 'friends' only. Your friends can already contact you through your account, so they'd have no reason to look you up by any other means.

- **Do you want search engines outside Facebook to link to your profile?**
  If you select yes for this option, it makes it possible for people to find your Facebook page by searching for your name on Google or any other search engine. For optimal security, select no.

  Now, head on over to your 'timeline and tagging' settings to finalize the process.

- **Who can post on your timeline?**
  To prevent strangers (and bullies) from posting on your timeline, you can set this to 'only me'. However, this will also prevent your friends from posting on your timeline.

- **Who can see what others post on my timeline?**
  Again, set this one to 'friends' or 'only me' so that strangers can't see the posts other people leave on your timeline.

  Avoid cyberbullies:

  If someone is using Facebook to harass you, you can block them from seeing your profile or contacting you. All you need to do is navigate to their profile and select the drop-down menu that's represented by three little dots at the top of their page. Then, select 'block'. They won't be able to find or view your profile, and they won't be notified that you have blocked them.

  Avoid inappropriate content:

  For the most part, Facebook's censorship software filters inappropriate and harmful content out of your feed. However, you can also set Facebook up to filter comments containing specific words out of your timeline.

Head back to your 'timeline and tagging' settings, and under the timeline category, select the 'hide comments that contain certain words' option. From here, you can create a list of words, phrases, and even emojis that you don't want to see on your timeline, and Facebook will block them for you.

Take a break:

You can log out of Facebook at any time, but for a more prolonged leave of absence, you can temporarily deactivate your account. All of your friends, posts, and photos will remain on your profile while you're away, but nobody else will be able to see your account or send you messages until the next time you login. This is a great solution if you need to take a step away from social media, but don't want to lose all of your content and memories.

To deactivate your account, go to settings > general > manage account > deactivate your account.

Twitter

What are some of the main risks on Twitter?

- Twitter is a hub for social and political activism, and sometimes, this can become overwhelming and distressing.
- Due to Twitter's diverse content, you may come across some explicit or triggering tweets from time-to-time.
- Passionate arguments often break out over Twitter discussions, and users may be at risk of experiencing cyberbullying.
- Like all social media, Twitter has the potential to become addictive and interfere with your everyday life.

Ways to protect yourself on Twitter

Make your tweets private:

When you set your Twitter profile and posts to private, they will only be visible to your followers. When someone new follows you, Twitter will send you a notification and you will be asked to approve their request, or deny it. However, accounts that

followed you before you protected your tweets will still be able to view and interact with your profile unless you block them.

To protect your tweets, head to the Tweet privacy section in your privacy and safety settings and check the box next to 'protect my tweets.' Click the save button, enter your password to confirm, and you're done!

Additionally, you can make it so that people who have your contact details aren't able to find you on Twitter unless you follow them first. From the privacy and safety settings page, uncheck both discoverability options.

Prevent Twitter posting your location information:

Every time you create a Tweet, you will be able to choose whether Twitter should post your location with it, or not. By default, Twitter won't share your location unless you have already opted in to the service.

Avoid cyberbullies:

Blocking someone on Twitter is similar to Facebook. From their profile, click the 'see more' icon (three vertical dots) and select 'block' from the menu. Then, click 'block' again to confirm. People you have blocked can't follow or see your Twitter profile. Twitter won't send them a notification when you block them, but if they visit your profile, they will receive a message informing them that they have been blocked.

Avoid inappropriate content:

The best way to ensure that you avoid content you don't want to see on Twitter is to only follow people who are already your friends, and only view content on your main Twitter feed. Once you delve into Twitter's search feature or investigate hashtags, you leave yourself vulnerable to inappropriate content. By default, Twitter will show a warning before you view content it deems as not safe for work, but this isn't 100% accurate as some content can slip through Twitter's filter.

Take a break:

Account deactivation on Twitter is a more permanent solution, so if you need to step away for a short while, it's better to log out. You could deactivate your account completely, but you face losing your profile and past tweets in the process.

Instagram

Make your account private:

When you're posting personal pictures on Instagram, privacy is important. You don't want strangers to be able to access your personal information or use your photos to impersonate you online

Luckily, you can make it so that all of your posts are private and only your friends can see them. To do this, head to your settings, then select account privacy and turn 'private account' on.

Now, people will need to send you a follow request, and you will need to approve it before they can see your posts, followers, and following lists. If someone was following you before you set your account to private and you don't want them to be able to see your posts anymore, you will need to block them.

Avoid cyberbullies:

Just like most social media platforms, Instagram makes it easy for you to block someone. All you need to do is go to their profile, hit the 'see more' button (represented by the little dots) and select 'block'.

Once you block someone, they can no longer find your profile, posts, or stories. Instagram won't notify people when you block them.

Avoid inappropriate content:

Although posting explicit content is against Instagram's policies, unfortunately, some users still share it. Similar to Twitter, the best way to avoid stumbling across explicit content is to stick with viewing the profiles of people who you trust and avoid exploring hashtags.

Time out:

If you're in need of a break from your Instagram account, login from a desktop or mobile internet browser, navigate to your profile, and click 'edit profile'. Select 'temporarily disable my account' and follow the prompts. All of your followers and content will remain until you're ready to log back in.

8 Online Dating and ASD

Online dating is a great avenue to meet new friends and potential romantic partners, but it brings with it some pretty serious dangers. People who you meet via online dating sites may not always be who they seem, and catfishing is rampant.

A 'catfish' is a person who creates an online dating profile through which they pretend to be somebody else. They might use a fake name, fake pictures, and a fake life story among other things to paint you a mental picture of the person they aren't.

It can be difficult to tell if someone is catfishing you, and so we delve further into how to check if someone is telling you the truth about their identity below.

If you're using the internet to date, remember:

- Always have a conversation with someone and get to know them before you agree to meet in person.
- Ask to speak with them over video chat, or on the phone to verify that they are the person in their pictures. Someone who is being honest about their identity will rarely have an issue with this and will take comfort in knowing you are, too.
- Also, ask if it is okay to add them on Facebook if you have an account. This way, you can check out their profile, pictures, and friends to get a clearer picture of who they are.
- Always agree to meet in a busy public space, like a cafe, during the day. Make sure there are people around who can help you if you get into trouble and consider asking a friend or family member to be situated
- Never tell them personal information like your address even if they are offering to pick you up.
- Make sure that you can get to and from the meeting place independently and safely. You don't want to be reliant on them for a ride home if you don't like them.

9 How to Tell if Someone is Who They Say They Are

Most of the people who you meet online will be genuine, but some will use fake profiles designed to draw you in and manipulate you. Luckily, you can usually verify if someone is telling the truth about their identity by using a few simple tricks.

Verify their picture:

Check to see if their profile picture is a real person.

If other photographs on their account show the same person, they may be telling the truth. You can save one of these photos to your computer and use Google's reverse image search to check if it appears anywhere else online.

If it appears in a lot of places, they may be using a stolen profile photo. But, if it only appears on their profile, chances are it is a photo of them.

Check their friend count:

Do they have any other friends on their account? If you are the only friend they have, they might be using a fake profile to target you.

If they have other friends, do the friends ever post anything to the person's timeline that might indicate they know each other in real life? If not, they could be using a fake profile to attract several targets who have never met them before.

Check their status updates and posts:

Are their status updates regular, everyday posts about their life? Or, are they mostly posting links and advertisements? If they are mostly posting links and ads, it is likely that they are using a fake profile to scam people or make sales.

Secrecy:

Have they told you not to tell anyone about them? If so, this indicates that they could have ill intentions and that they are not a genuine friend.

Money:

Have they asked you for money, or told you they are in a bad situation and need help with money? If so, they are likely posing as a friend in order to scam you.

If you suspect that your online friend isn't who they claim to be, you should stop talking to them and block their account.

10 **Signs that Something Might be Wrong Online**

If you feel upset, uncomfortable, or unsafe, something might be seriously wrong with your online situation. It's important that you listen to this inner feeling and leave the situation before it goes too heavy. You may need to block the person who is making you feel unsafe, or seek help from a third party, like a family member or the police.

If one of **your online friends** is saying something one day and then contradicting it the next, it's possible that they aren't being truthful about their identity. You could use the steps listed above to see if everything checks out, and if it doesn't, you may need to make the decision to remove them from your online circle.

Cyberbullying is common on social media, and if someone is being cruel to you or other people, they aren't worth your time. You should report their cruel comments to the website's administrator and then block them to prevent them from contacting you in the future.

If something seems too good to be true, then it probably is. You should always be cautious of scams. Remember that if a stranger or friend is offering you something that sounds a little fishy, like a prize for clicking on their link, you should avoid it at all costs. If you're unsure, you can search on Google or even Snopes to find out if it is a scam.

11 Ways to Improve Your Child's Internet Safety

Protecting a child from the dangers on the internet should be a concern for all parents, even more so if they have children on the Autism spectrum. We've put together the following tips as a guide to keep your children safe online and avoid some of the dangers that can be found online.

- Keep your family's computer in a communal space, like a lounge room or in the kitchen. This way, you can check in regularly and keep an eye on what's happening in your child's online social circles.
- Create some visual reminders and posters of internet safety tips and hang them up in the room around your computer. This can be a great opportunity to sit with your child and discuss internet safety while coming up with some rules together.
- Educate your child about online safety, clarify that they understand, and renew their knowledge regularly.
- Roleplay different scenarios with your child to teach them how to react to online dangers in a safe setting. You could create an account on the platform they're using, and use this to send them messages as part of the roleplay to make it seem more realistic.
- Write and enforce a strict roster around internet usage times to avoid complications with internet addiction. You may even divide time spent online into separate categories, like play or study, and work that into the roster as well.
- Put all electronics away about two hours before bed to help improve your child's sleep.
- Use internet content filters, like Net Nanny, to monitor and restrict your child's browsing activity. These programs will also restrict their access to inappropriate content, and any other websites you block.
- Install child-friendly internet browsers like KidSplorer – they are visually appealing to children, and they make it safer for them to use the internet. Similar to a content filter, they'll only be able to access the websites you have specified and will even block access to the internet at predetermined times.
- Establish a plan with them on what they should do if they encounter a cyberbully, how they should react, and who they should tell.
- Casually ask them about their online friends and what they've been talking about, similar to the way in which you'd ask them how their school day went.
- Provide them with a checklist of the information that they are not allowed to give out over the internet, such as their full name, birth date, address, and school name.

12 Conclusion

In summary, the key here is to ensure you're internet safe. Focus on incorporating tighter online security measures and heightened safety precautions. Educate yourself, be vigilant and be aware.

> Those with ASD are more susceptible to online threats than others, so it's even **more important to follow our advice for remaining safe online**.

Cyberbullies and online scammers will unfortunately always have a place online, so it's your job to stand up and take the necessary steps to protect yourself from attack.

Follow our steps so you can spot when something is not right and take action to protect yourself when you feel threatened.

This **Internet Safety Guide** has flagged the **key areas you should watch out for**, and how to tackle the threats faced. Enjoy your time online, but remember to be internet safe and careful at the same time!

WRITTEN BY **Gray Williams**

Gray Williams is an experienced data and communications engineer and cross-platform copy and content writer and editor with a keen interest in cybersecurity. He has been working with and researching, VPNs and other online privacy tools for many years.