



|
**ONLINE
SAFETY
SKILLS**

**STRATEGIES &
TIPS MANUAL**

**A COMPREHENSIVE
COLLECTION OF
ONLINE INFORMATION
FOR INDIVIDUALS
WITH AUTISM**

|
4.2023



pennsylvania
DEPARTMENT OF HUMAN SERVICES

TABLE OF CONTENTS

CHAPTER	PAGE
1. <u>GENERAL TIPS AND STRATEGIES</u>	4
<u>Understanding online lingo and terms</u>	4
<u>Online Readiness Checklist</u>	4
<u>General proactive tips & strategies to safeguard your computer & online accounts</u>	6
<u>How to check if a website is secure</u>	8
<u>Create strong passwords</u>	8
<u>Safe Web Browsing</u>	10
<u>Legal consequences of online activities</u>	11
<u>Signs that something might be wrong online</u>	12
<u>Guide to what’s illegal to view on the internet</u>	13
<u>Is there anything that can be done, if you are a victim of an internet crime?</u>	15
<u>Consider lack of confidence</u>	15
2. <u>TIPS & STRATEGIES FOR SPECIFIC PLATFORMS</u>	20
<u>Cellphone (Smartphone) security risks</u>	20
<u>iPad security risks</u>	22
<u>Mac security risks</u>	24
<u>Protection on social networks</u>	32
<u>Twitter</u>	33
<u>Facebook</u>	37
<u>Instagram</u>	39
<u>Snapchat</u>	40
<u>Protection on gaming sites</u>	41
<u>Understanding parental controls on gaming sites</u>	43
<u>Protection on online dating sites</u>	44
3. <u>TIPS & STRATEGIES FOR SPECIFIC RISKS</u>	47
<u>Digital and sensory overload</u>	47
<u>Addiction</u>	48
<u>Scams, manipulation or hacking</u>	49
<u>Online Misunderstandings</u>	50

	Online dating and romance scams	50
	Catfishing & Sextortion	52
	Phishing emails	59
	Cyberbullying	60
	Pornography	62
	Legal traps for internet pornography users: 5 ways you can get in trouble	62
4.	<u>TIPS & STRATEGIES SPECIFICALLY FOR CHILDREN, TWEENS &</u>	
	<u>TEENS</u>	65
	Although these are designed for children and teens, these resources can be used with adults, depending on their level of knowledge, and understanding. A number of these resources can be generalized to other ages and populations as well.	
	General tips & strategies specifically for families with children and teens	65
	Common internet safety rules for children and teens	65
	PLAY IT SAFE acronym to teach teens with ASD about internet safety	66
	Exposure to inappropriate content	68
	Online luring	69
	Self/ peer exploitation	70
5.	<u>TOOLS, RESOURCES & GAMES FOR TEACHING ONLINE SAFETY SKILLS</u>	74
	Workbooks and Curriculums	74
	Tools and Resources	74
	Games	76


Online Safety Skills

Strategies & Tips Manual

Online safety has always been a threat to individuals. However, this has dramatically increased over the last couple of years as a result of the pandemic, social distancing and changes in work practices. Although protection and security need to be considered by everyone, there are specific populations that are more vulnerable than others.

Pennsylvania's Office of Developmental Programs has created this safety manual, which contains tips and strategies for individuals, supporters and families to use in an effort to decrease risks associated with internet use. It is a comprehensive collection of information found on countless websites and addresses a wide range of online safety concerns. It is intended to maximize awareness and provide options for support to those who need it most.

SPECIAL NOTES:

- **The websites that the information has been collected from are referenced to ensure the developers are provided the proper credit.**
- **Any information specific to [autism](#) or [disabilities](#) is highlighted with a  sign in the margin for ease of identification.**
- **If you are a provider for an individual who is receiving waiver services, be sure to consult with the team prior to implementing these strategies. Some strategies may be considered restrictive and must be approved by a human rights team before being implemented.**

GENERAL TIPS & STRATEGIES

Understand online lingo and terms

It is beneficial to understanding the language and acronyms used online, both as the person interacting with others as well as the parent and or supporter of that person.

It can help:

- the person to recognize potential threats
- others to identify if there is a need for concern
- parents who want to keep up with what their? children are talking about

[Netlingo](#) is an online dictionary of thousands of internet terms, words and acronyms to empower people to understand the internet and have another level of protection from risks.

Online Readiness Checklist

The following information has been taken from [Online Readiness Checklist — PAAutism.org, an ASERT Autism Resource Guide](#)



The purpose of this checklist is for supporters to plan for **autistic** individuals who are participating in online communities so they can be as safe and prepared as possible.

When we say “online,” we mean a broad spectrum of internet activities: visiting websites, texting, instant messaging, chatting, email, video conferencing, watching videos, online gaming, reading blogs, online purchasing, looking for info (e.g., health, news, activities), and social media through the use of smartphones or other internet-enabled devices.

Answer “yes” or “no” to the questions below to help determine areas that might indicate a person is/isn’t ready to participate in online communities.

IS THE INDIVIDUAL ABLE TO COMPREHEND AND INTERPRET SOCIAL CUES AND SIGNS ONLINE OR VIRTUALLY?



Autistic individuals may have difficulty interpreting non-verbal aspects of behavior and non-literal aspects of speech, such as sarcasm, humor, metaphors, or euphemisms.

- **Consider the following when answering this question:** understanding and using emojis, understanding when an online conversation is done, understanding warning signs, such as “graphic image,” “Rated X,” “for individuals age 18 or older,” etc.

IS THE INDIVIDUAL ABLE TO DECIPHER CREDIBLE SOURCES THAT THEY FIND ONLINE?

Individuals on the spectrum may have challenges with differentiating what is a safe source to engage with. This can be especially problematic as there are often scammers on the internet or emails, false advertising, click bait ads, and lack of credible information being shared.

- **Consider the following when answering this question:** differentiating opinion versus fact, most used sources of information, does the individual accept all information shared as fact, etc.

IS THE INDIVIDUAL ABLE TO DETERMINE WHO IS A TRUSTWORTHY PERSON ONLINE?

Because there is a layer of anonymity online, the person on the other side of the conversation may not be who they say they are and could take advantage of the individual or get them into trouble.

- **Consider the following when answering this question:** do they do things to please others/avoid confrontation, have they been victimized/taken advantage of, have they received mean or harmful content and whether they know what to do, have they received unwanted attention (e.g., request for personal information or photo) and know what to do, ability to verify friendships online, being aware of and skeptical of information that people can learn online about them, cautiousness of strangers or unknown situations, do they ask questions about who is contacting them, do they have a trusted person they share information with like who they are speaking to online, do they verify contact information before reaching out (ex. texts, calls, emails from bank), etc.

IS THE INDIVIDUAL ABLE TO CONTROL IMPULSIVE BEHAVIORS?

With instant access to all the information, items/goods, services, images, etc. online, the internet may be challenging for individuals with impulsive thinking or behaviors. This could lead to clicking on something inappropriate or illegal, disclosing personal information, spending excessive amounts of money, etc.

- **Consider the following when answering this question:** excessive use of internet (e.g., social media), impulsive buying (e.g., making unplanned purchases), excessive video gaming, often swear or use offensive languages on the site/when commenting, a lack of control of screen time

IS THE INDIVIDUAL ABLE TO SPEND/MANAGE MONEY ONLINE MOSTLY INDEPENDENTLY?

The internet can be a problematic place for even those who are mostly independent with managing their money. With quick ways to pay, spending can be one click away. Such ease with paying for items, services, or in-app purchases can quickly add up and become an unexpected costly expense.

- **Consider the following when answering this question:** level of independence with money management, correctly using credit/debit cards, regularly checking bank statements or credit card balance, ability to save/plan for expenses, ease of spending unknowingly spending excessive amounts of money online (e.g., for games, fashion, gambling), do they have trouble saying no when someone asks for help, knowledge of what to do if financial information is compromised, etc.

IS THE INDIVIDUAL ABLE TO SAFEGUARD SENSITIVE INFORMATION ONLINE?

While sensitive information can be securely sent online, not all sites or people who are encountered online are trustworthy. For individuals on the spectrum, deciphering when and when not to share personal information may be more challenging.

- **Consider the following when answering this question:** awareness of what is private or sensitive information, ability to recognize a secure vs non-secured website, knowledge of public vs private

Wi-Fi connections, awareness of who can access private information via social media, knowledge of how to safely keep track of login information, know not to share their login information, awareness of how much information to share in public profiles (ex. TMI in dating profiles), does the individual know what to do if private information has already been shared (where to report), etc.

IS THE INDIVIDUAL ABLE FOLLOW RULES AND LAWS REGARDING ONLINE ACTIVITY?



It is important to consider how well an individual recognizes what is acceptable and what is problematic, and sometimes illegal, behaviors. With **autism**, there may be a lack of awareness for what is appropriate and inappropriate behaviors online. This can be especially true for individuals with interests that are uncommon for their age group. For instance, an adult who has an interest in a children's show may be accessing websites generally intended for children and may communicate with children, which can be concerning.

- **Consider the following when answering this question:** understanding of which sites are appropriate for them (e.g., children's website), interest that could lead to inappropriate interactions/websites, right and protection of others' privacy (e.g., personal emails, electronic medical records, etc.), sending or posting mean or harmful content of someone, knowing what to do when someone else is bullied online, in a relationship versus seeking relationships online, interest in same age/appropriate age peers, etc.

General proactive tips & strategies to safeguard your computer & online accounts

The following information has been taken from [On the Internet: Be Cautious When Connected — FBI](#), [Safety online: A guide for people with autism spectrum disorder \(openmindschool.org\)](#), and [#3: Are Autistic People More Vulnerable to Cyber Attacks? \(linkedin.com\)](#)

Everyday tasks such as opening an email attachment, following a link in a text message, making an online purchase; can open you up to online criminals who want to harm your systems or steal from you. Preventing internet-enabled crimes and cyber intrusions requires each of us to be aware and on guard.

PROTECT YOUR SYSTEMS AND DATA

- Use a **firewall**
- Keep your **antivirus software** up to date
- **Shut down** computer when you are not using it
- Keep systems and software up to date and install a strong, reputable anti-virus program.
- Create a strong and unique **passphrase** for each online account you hold and change them regularly. Using the same passphrase across several accounts makes you more vulnerable if one account is breached.
- Do not open any **attachments** unless you are expecting the file, document, or invoice and have verified the sender's email address
- Ensure you are familiar with the **email address** that sent you a message before clicking on any links or opening attachments
- Protect your cell phone by setting software to update automatically. These **updates** could give you critical protection against security threats.

- Protect your accounts by using **multi-factor authentication**. Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.
- Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:
 - something you know — like a passcode, a PIN, or the answer to a security question.
 - something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key
 - something you are — like a scan of your fingerprint, your retina, or your face
- Protect your data by backing it up. **Back up the data** on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.
- Use a **password manager** to ensure that all your accounts aren't compromised in a data breach, it helps to use complex and unique passwords for each account. Rather than remembering each of them, password managers let you store those logins in an encrypted database. That way, you only have to remember one password.
- Use new and updated versions of **web browsers** (e.g., run Internet Explorer 11 instead of 6), Some alternative browsers collect and store personal information, addresses, ad even credit card numbers that can easily be hacked and accessed.
- Change the settings that control the types of personal information the web browser will save:
- Change the **“cookies”** setting based off of your preferred level of security as well as to delete the cookies when not needed.
- Change settings to delete your web browser's **cache** often and when you close the browser.
- Install add-ons to block **scripts** from running. It is recommended to block scripts for all sites except for those that you trust.

PROTECT YOUR CONNECTIONS

- **Be careful when connecting to a public Wi-Fi network** and do not conduct any sensitive transactions, including purchases, when on a public network.
- **Avoid using free charging stations in airports, hotels, or shopping centers.** Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices that access these ports. Carry your own charger and USB cord and use an electrical outlet instead.

PROTECT YOUR MONEY AND INFORMATION

- **Examine the email address in all correspondence and scrutinize website URLs.** Scammers often mimic a legitimate site or email address by using a slight variation in spelling. Or an email may look like it came from a legitimate company, but the actual email address is suspicious.
- **Do not click the link in an unsolicited text message or email that asks you to update, check, or verify your account information.** If you are concerned about the status of your account, go to the company's website to log into your account or call the phone number listed on the official website to see if something does in fact need your attention.
- **Carefully scrutinize all electronic requests for a payment or transfer of funds.**
- **Be extra suspicious of any message that urges immediate action.**

- **Make online purchases with a credit card for an extra layer of protection against fraud.**
- **Do not send money to any person you meet online or allow a person you don't know well to access your bank account to transfer money in or out.**

How to check if a website is secure

The following information has been taken from [The Ultimate Online Safety Guide for People with Autism / Spectrum Disorder](#)

There are several ways to tell if a website is secure or not:

- **Look for HTTPS in the URL bar.** This indicates that the page was loaded securely using SSL/TLS encryption technology.
- **Check the lock symbol next to the URL bar.** The lock symbol appears only after a webpage has been encrypted with TLS.
- **Click the padlock icon in the browser toolbar.** If it opens, then the connection between your browser and the server is secured. Otherwise, there might be something wrong with the security settings.
- **Use a security tool.** There are many third-party applications available that will scan sites for vulnerabilities and help identify potential threats.

Create strong passwords

The following information has been taken from [Internet Safety: Creating Strong Passwords \(acfglobal.org\)](#)

You'll need to create a password to do just about everything on the Web, from checking your email to online banking. And while it's simpler to use a short, easy-to-remember password, this can also pose serious risks to your online security. To protect yourself and your information, you'll want to use passwords that **are** long, strong, and difficult for someone else to guess while still keeping them relatively easy for you to remember.

- Watch [this video from Safety in Canada](#) to learn more about creating a strong password.

WHY DO I NEED A STRONG PASSWORD?

At this point, you may be wondering, why do I even need a strong password anyway? The truth is that even though most websites are secure, there's always a small chance someone may try to access or steal your information. This is commonly known as hacking. A strong password is one of the best ways to defend your accounts and private information from hackers.

TIPS FOR CREATING STRONG PASSWORDS

A strong password is one that's easy for you to remember but difficult for others to guess. Let's take a look at some of the most important things to consider when creating a password.

- **Never use personal information** such as your name, birthday, user name, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.

- **Use a longer password.** Your password should be at least six characters long, although for extra security it should be even longer.
- **Don't use the same password for each account.** If someone discovers your password for one account, all of your other accounts will be vulnerable.
- **Try to include numbers, symbols, and both uppercase and lowercase letters.**
- **Avoid using words that can be found in the dictionary.** For example, swimming1 would be a weak password.
 - **Random passwords are the strongest.** If you're having trouble creating one, you can use a [password generator](#) instead.

COMMON PASSWORD MISTAKES

Some of the most commonly used passwords are based on family names, hobbies, or just a simple pattern. While these types of passwords are easy to remember, they're also some of the least secure. Let's take a look at some of the most common password mistakes and how to fix them.

- **Password: brian12kate5 (name and age of your children)**
Problem: This password uses too much personal information, along with common words that could be found in the dictionary.
 - *Solution:* A stronger version of this password would use symbols, uppercase letters, and a more random order. And rather than using family names, we could combine a character from a movie with a type of food. For example, Chewbacca and pizza could become **chEwbAccAp!ZZa**.
- **Password: w3St! (your street address)**
Problem: At only five characters, this password is way too short. It also includes part of her address, which is publicly available information.
 - *Solution:* A stronger version of this password would be **much longer**, ideally more than 10 characters. We could also substitute a nearby street name instead of her current address. For example, Pemberly Ave could become **p3MberLY%Av**.
- **Password: 123abcba321 (you consistently follow a simple pattern)**
Problem: While patterns like this are easy to remember, they're also some of the first things a hacker might guess when attempting to access your account.
 - *Solution:* Remember that **random passwords** are much stronger than simple patterns. If you're having trouble creating a new password, try using a [password generator](#) instead. Here's an example of a generated password: **#eV\$plg&qf**.

 If you use a password generator, you may also want to create a **mnemonic device** to make the password easier to remember. For example, **H=jNp2#** could be remembered as **HARRY = jessica NORTH paris 2 #**. This may still feel pretty random, but with a bit of practice it becomes relatively easy to memorize.
- **Password: BrAveZ!2 (you use the same passwords for all accounts)**
Problem: There's nothing really wrong with this password, but remember that you should **never use the same password with different accounts**.

- *Solution:* Create a unique password for each of your online accounts.

USING PASSWORD MANAGERS

Instead of writing your passwords on paper where someone might find them, you can use a **password manager** to store them securely online. Password managers can remember and enter your password on different websites, which means you won't have to remember longer passwords. Examples of password managers include [LastPass](#), [1Password](#), and [Google Chrome's password manager](#).

- **Password: M#p52S@AP\$V (developed using a password generator and different from all other accounts)**

This is a great example of a strong password. It's strong, long, and difficult for someone else to guess. It uses more than 10 characters with letters (both uppercase and lowercase), numbers, and symbols, and includes no obvious personal information or common words. This password might even be a bit too complicated to remember without a password manager, which underscores why they're so helpful when creating a strong password.

Remember to use these tips whenever you create a password to keep your online information safe and secure.

Safe web browsing

The following information has been taken from [Safe Web Browsing | RAINN](#)

When you want answers, chances are you're going to look online. According to a recent study from the [Pew Research Center](#), 72 percent of Internet users say they looked online for health information within the past year. People affected by sexual violence also turn to online resources for support. Whether you are looking for help for yourself or someone you care about, there are two important safety elements to consider: privacy and security.

PRIVACY: USE PRIVATE BROWSING, DELETE ACTIVITY, OR USE ANOTHER DEVICE

Your browser downloads and stores a record of the webpages you visit on your computer or device. This is called a web history, also known as a browser cache. There are times when you may want conceal your activity online for safety reasons. There are a few ways to accomplish this:

- **Use private browsing.** Most browsers have a privacy mode that allows you to visit websites without storing any record of your activity on your computer or device. Learn more about private browsing:
 - *Google:* Incognito Mode
 - *Firefox:* Private Browsing
 - *Internet Explorer:* InPrivate Browsing
 - *Safari:* Private Browsing
- **Clear your cache, history, and cookies.** If you visited a site without privacy mode, you can erase records of your activity by clearing your cache, history, and cookies on your computer or device. Keep in mind that if someone is actively monitoring your computer, erasing this data could alert them to the fact that you are trying to conceal your actions.

- *Mozilla Firefox*: delete browsing history, clear cache, and delete cookies
- *Internet Explorer*: delete browsing history and delete cookies
- *Google Chrome*: delete browsing history, clear cache, and delete cookies
- *Safari*: privacy support
- **Use another device.** If you believe your computer or device is being monitored or isn't safe, consider using a computer from a friend or a public library. You can find the nearest library by visiting PublicLibraries.com

SECURITY: LOOK FOR “HTTPS” AND ENCRYPT YOUR DATA

The more ways you connect online, the more opportunities you have to protect your information and the information you share with others.

- **Use secure sites.** Verify that a site is secure by looking for “https” at the beginning of the URL or the small lock icon that appears in the web address bar. These symbols let you know that the site has been encrypted, meaning that your visit to this site hasn't been intercepted by another computer. If you don't see either security symbol, be cautious about information you share on that site. Some sites use “http,” which is not secure.
- **Encrypt your data.** Even if a site uses https, the hosts of that site can often still access your data. For example, messages and pictures that you've sent over an email service could be viewed by the company who run this service. You can choose to use services that encrypt your data before sending it to the cloud.
- **Review your syncing settings.** If you share a device with someone, look into the settings on your devices that control what information is copied to the cloud. For example, if you visited a website in Google Chrome on your mobile device, it might be listed in the history on your desktop or laptop computer. You can adjust syncing settings to limit what information can be accessed by different devices. If you're concerned with someone monitoring your activity, use private browsing mode.

YOU CAN REPORT INAPPROPRIATE IMAGES.

If you see or receive inappropriate sexual images online, you can report it to police or through CyberTipline.org. Cyber Tipline “receives leads and tips regarding suspected crimes of sexual exploitation committed against children.” Child pornography is a crime. If you encounter these images online, you can play a role in having them removed and holding perpetrators accountable.

To speak with someone who is trained to help, call the National Sexual Assault Hotline at 800.656.HOPE (4673) or chat online at online.rainn.org.

Legal consequences of online activities

The following information has been taken from [What Are Possible Penalties for a Cyber Crime in Pennsylvania? - The Fight for Religious Freedom in the Military Continues \(yountslaw.com\)](#)

Some of the activities engaged online can in fact have legal consequences. Individuals may be unaware certain behaviors and actions can be deemed a criminal offense. It's also important to educate them

before they get into these situations so they understand some of the Pennsylvania laws pertaining to online victimization.

BELOW ARE SOME PENNSYLVANIA LAWS INVOLVING ONLINE VICTIMIZATION:

- **Online harassment** is a misdemeanor of the third degree. This involves engaging in conduct that harasses or annoys another person via e-mail or the internet. The penalty is up to one year in jail and fines of up to \$2,500.
- **Online stalking** is a misdemeanor of the first degree if it's the first violation. It occurs when someone repeatedly communicates with another through the internet or e-mail to the extent of causing the recipient emotional distress or reasonable fear of bodily harm. The penalty is up to five years imprisonment and fines of up to \$10,000.
- **Computer trespass** is a third-degree felony in Pennsylvania. It occurs when a person unknowingly or knowingly gains access to a computer, data, or network and changes or deletes data without authorization. A conviction carries up to seven years in prison and fines of up to \$15,000.
- **Computer theft** is a third-degree felony and carries up to seven years imprisonment and fines of up to \$15,000.
- **Unlawful use of a computer or e-mail** is a felony of the third degree. It involves accessing or exceeding the permissible use of a computer, program, network, system, database, website, or any computer-related thing to disrupt normal function or defraud them. The punishment is seven years' imprisonment and fines up to \$15,000.
- **Online child pornography** is a third-degree felony involving possessing or intentionally viewing a computer with a child under 18 engaging in sexual acts. A first offense will attract up to seven years in prison and fines of up to \$15,000.

The charges can also escalate for subsequent convictions. Similarly, online stalking or harassment towards family members may be considered domestic offenses and can affect your child custody rights or ability to work in certain jobs.

Online sex-related offenses may also make you a registered sex offender, which the public could see. The harshness and extent of repercussions you could face should prompt you to seek the legal guidance of an experienced and skilled cybercrime defense lawyer, immediately.

Signs that something might be wrong online

The following information has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)

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 within

this handbook 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.

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.

Guide to what's illegal to view on the internet

The following information has been taken from [Think Before You Click! Guide To What's Illegal On The Internet \(nonstopjustice.com\)](#)

There are over four billion global internet users. Everyone uses the internet for different reasons — while some enjoy looking at cat pictures, others are building their startup using internet tools. In this article we'll look at what is illegal to view on the internet.

While the internet has many benefits, it can be a medium for obscene content.

If you view this kind of content, tracking you down is easier than you think. Law enforcement agencies are quick to arrest anyone who views illegal content online — even if you unintentionally stumbled upon these websites.

But do you mean what's considered legal and what's considered illegal? Read on to know what is illegal to view on the internet.

TORRENTING

Torrenting is a type of file sharing conducted between different users on the internet. Torrenting usually involves a platform where one individual uploads illegal content, such as a copyrighted film or song, and others are free to download this material.

Torrenting has decreased in the last few years. Streaming powerhouses such as Netflix make entertainment consumption affordable and easy, preventing the need to download pirated material.

Can you actually get arrested for torrenting? While torrenting is illegal, few arrests have actually been made. But there are repercussions, even if it's simply a warning letter or restricted internet access.

CHILD PORNOGRAPHY

Child pornography charges and arrests happen every week in every part of United States.

Child pornography is defined as sexual and exploitative actions featuring minors under the age of 17. This type of content includes both images and videos. Possessing both can lead to arrest and serious legal consequences.

Individuals not only get arrested when viewing child pornography but may get arrested for merely searching for child pornography online. This also includes searching for such content on the "dark web."

Authorities keep a record of search terms and track IP addresses that trigger certain keywords. If the search term appears in your browser history and cache, authorities may suspect you of watching child pornography.

CRIMINALS FOR HIRE

The dark web is known as the criminal world of the internet. This part of the internet isn't indexed by search engines, giving users anonymity. This is why you'll find many examples of criminal activity on the dark web, including hiring someone to conduct an illegal act on your behalf.

Hiring someone to hurt, injure, or do harm to another person is illegal. If law enforcement catches someone engaging in such criminal contracting, they could be apprehended and face significant charges.

TERRORISM

The internet can be a tremendous resource to spread ideas and connect individuals from all over the world. Unfortunately, terrorist ideas are easily spread globally, inspiring others to act out violently.

While searching for news articles or fictional novels depicting terrorism is fine, these searches can still alarm the authorities. If they suspect you may be a terrorist, you could be arrested.

Some specifics include joining online terrorist organizations, making threats, or encouraging others to engage in terroristic acts. Even some searches about weaponry or explosive devices could draw the attention of authorities.

EXPLOSIVE TERMS

One of the easiest ways to track down someone suspected of a terrorist attack is tracking weapon-related search terms, such as making homemade explosive devices.

This is especially true if you're searching for homemade bombs disguised as everyday items (such as a backpack).

Even if an arrest isn't made, law enforcement can put you on their watch list and will track your IP address closely. You may even have law enforcement officials showing up at your door.

MODIFYING WEAPONS

While owning weapons such as guns are legal in many parts of the US, Certain modifications are against the law in some areas.

Bump stocks are the perfect example. They combine two different parts: a plastic stock and a firearm. The bump stock harnesses the recoil of a rifle to accelerate trigger pulls.

Searching for weapon modifications such as bump stocks can put you on a watch list. Weapon modifications can result in hefty fines and serious jail time.

MURDER SHE WROTE

Not every search for murder will result in an arrest.

For example, let's say you're a fan of murder mystery films and novels or you're searching for more information about a recent murder in your area. These usually aren't a reason to put you on a watchlist.

But certain murder-related terms will alarm authorities. These include how to commit a murder, how to clean up after a murder, and other related terms.

ILLEGAL DRUGS

Buying drugs online is more common than you think. If you try to buy drugs online, whether on the surface or deep web, you'll attract attention from the authorities.

Keep in mind, searching for terms related to illegal drugs likely won't put you on a watchlist. These terms include "how to detox from heroin" or "how many people use cocaine."

But terms relating to finding or purchasing these drugs may raise alarm bells.

ANOTHER INDIVIDUAL'S PROPERTY UPLOADED WITHOUT THEIR PERMISSION

Did you know sharing another individual's property online without their permission is illegal? "Property" can be defined as images, videos, and words. For example, it's illegal to film someone without their knowledge and upload it online.

What if you view this content, not knowing it's illegal? You might not get arrested — however, the uploader could face serious charges.

WHAT IS ILLEGAL TO VIEW ON THE INTERNET? BE CAREFUL WHEN SURFING THE WEB

Many may wonder, what is illegal to view on the internet? We all know viewing and downloading child pornography can result in an arrest. But even searching for specific terms can put you on the internet watchlist and can even result in an arrest.

That's why it's important to be careful when on the internet. This includes downloading pornography, unaware that minors were involved in the pornographic content you were watching.

Is there anything that can be done, if you are a victim of an internet crime?

The following information has been taken from www.ic3.gov

Anyone can become a victim of internet crime. Take action for yourself and others by reporting it. Reporting internet crimes can help bring criminals to justice and make the internet a safer place for us all.

Reports can be submitted at the *Internet Crime Complaint Center (IC3)* at www.ic3.gov

Consider lack of confidence


The following information has been taken from [Autism and the internet: risks and benefits](#)

Ledingham and Mills (2016) suggest financial gain is not the hacker's motivation.

It is:

- attention
- adulation

- self-satisfaction
- recognition

 These factors suggest low confidence, something often found in young **autistic** adults (Howlin, 1997).

STRATEGIES TO HELP BUILD SELF-ESTEEM

The following has been taken from [10 Tips to Improve Autistic Confidence & Self-Esteem - Autistic & Unapologetic \(autisticandunapologetic.com\)](https://autisticandunapologetic.com)

- **Pick your Battles**

Confidence can often feel like rolling a big old boulder. When it's going well, we have great momentum and things only seem to get easier but, when we hit a bump, we can see our confidence greatly decrease – which, for **autistic** people who tend to over analyze, can be a particular problem as we usually dwell that extra bit longer on any blows to our self-esteem.



- To avoid retreat which this can cause, **autistic** people should be encouraged to try and get their confidence boulder rolling early. **This can be done by building up a momentum with a series of smaller/similar experiences first.** For example, if an **autistic** person freezes up in crowds, start with short meetings where the number of people they do know outweigh those they don't.
- Alternatively, it's fully justified to avoid an overly hazardous event if you feel it will do more damage in the long run. However, before you do call in to say that your dog ate your desire to show up, **consider whether you are really doing this because you believe it will help or whether it's just plain old jitters getting the better of a situation.**

- **Build new skills**

If we consider that confidence is self-belief in our skills and abilities, then it's unquestionable that, for those who are currently lacking in it, picking up a new skill or ability can help improve it. This can come in the form of joining a club or starting a new hobby – ideas for which can be found in my 2 **autistic** hobbies, activities and sports articles, which include highlights such as:



- Drawing
- Swimming
- Trampolining
- Yoga
- Chess
- Dungeons & Dragons
- [read the full articles [here](#) and [here](#)]

Of course, whilst the range of options might at first seem overwhelming (and you may even pick the wrong choice first time around), once you do find something you can sink your teeth into, the benefits are visible almost immediately, as we cut our teeth on meeting and interacting with people in a situation where we don't have to rely on words (was that too many 'teeth' metaphors?).

Nevertheless, it should be worth noting that, when picking up any new skill like this, **there will always be a learning curve** – which at some point or another can work to pit us against the enjoyment of these new experiences. So, when this does happen, try not to be deterred, as

quitting at these pivotal points can make us drop further than we may have grown and lead to a dangerous ‘I’m not good enough’ mindset.

- **Celebrate Every Achievement**

Confidence is unquestionably born out of success. However, for far too many autists successful experiences seem few and far between. Over time, this can lead to a diminished opinion of our abilities and achievements; a domino effect which ultimately hurts our confidence.



Helping **autistic** people to recognize that this need not be the case is therefore crucial in reclaiming a reason to stand up straight – something which is made a lot easier by encouraging **autistic** people to **share/discuss/remember 3 things they are proud to have done each day**.

These three things can range from anything as large as climbing Mount Everest to just remembering to water a plant, as it’s not the action of remembering the achievement that will put some pep in your step but the realization of all we can and do achieve.

On the note of recording your wins, I always encourage people to document these in a book as few things will give you quite the ego boost as being able to get to the last page and realize you have filled an entire book with your greatness.



- **Learn to say ‘Yes’**

While your comfort zone may well and truly be, erm, comfortable, it’s not always in your best interest to reside there for too long. This is because, while comfort zones do offer a nice respite for the active **autistic** mind, they also pose 2 larger risks to our confidence which are rarely worth the relaxation:

- Any confidence you do develop will be fragile, as it is purely built around what you know and not what you don’t.
- While we all grow in some way each day, safe havens forever stay the same size, making them feel cramped over time and eventually leaving no room for others.

By learning to say ‘yes’ to new opportunities, these issues can be avoided, giving us valuable experiences to develop our confidence in a broad range of scenarios. Whilst at first you would think that this means saying bon voyage to our beloved comfort zones, what you will quickly realize is that the new can itself become comfortable, **changing this safety vacation into more of a comfort zone extension**.

If you support someone, teaching someone to say ‘yes’ is more about learning not to take ‘no’ as an immediate response. For example, if most questions are constantly met with rejection, try to understand their reasoning and look for a middle ground, which feels more like something they decided on (rather than something you had to negotiate out of them).

- **Learn to say ‘No’**



On the other side of the coin, **autistic** confidence can often sink faster than the Titanic if we feel that we are constantly being led into decisions which are made by others. This can be a problem for **autistic** people as, despite our mind’s unique way of thinking (or perhaps, in spite of it), we can often get caught in the pack listening to others and afraid to stand out by sharing alternative views.

- ⊕ That’s why learning to say ‘no’ in moderation can be a powerful tool for **autistic** people as, in two simple letters, you are taking back control of what others want and also avoid the awful possibility of **autistic** manipulation (more of which can be read on [here](#)).
- ⊕ Once again, for those who are supporting **autistic** people, this one is a little bit trickier, as telling someone to say no is somewhat of a Catch 22 (where they would have to say ‘yes’ to take your advice). So, instead of encouraging the word ‘no’, start asking your loved one what they think about events or choices and if they’re not happy with it, then say that they don’t have to do it, but they have to take control by selecting a substitute activity.
- **Overcome Imposter Syndrome**
 - ⊕ Many **autistic** people struggle to feel confident in situations, as we often feel like we don’t deserve to be there (in fact, for some **autistic** people we even feel at odds in our own community, as we aren’t an exact match for the examples of the spectrum we see). This state of mind, which gives us an inability to recognize our value, is known as Imposter Syndrome and, whether it’s holding us back at work or with friends, it’s incredibly damaging for our confidence.

Although not true for everyone, it’s often the case that we develop Imposter Syndrome by inaccurately comparing ourselves to those around us. A few years ago, this was only a minor issue, but with the advent of social media (where everyone is constantly perceived as living their best life), this has become more prevalent as we falsely believe that those we surround ourselves with are better than us, or we end up having to push lies ourselves which only makes us feel more false.

Taking social media breaks can be a great way to avoid this and, if you use the time to talk to people about your insecurities, these hiatuses will often lead to some great realizations like:

 - You’re underselling yourself.
 - Everyone gets imposter syndrome at some point – except, ironically, actual imposters themselves.
 - **Find A Confident Frame of Mind**
 - ⊕ We’ve come a long way since the days that we thought all autists were incapable of empathy. In fact, we’ve come so far that we now no longer see **autistic** people as having too little emotion but way, way too much.
 - ⊕ This can be seen in how **autistic** people seemingly absorb any feelings within the room we enter, making the spectrum somewhat of an emotional sponge for hope, optimism and any of the other emotions which inspire confidence in people – see where I’m going here?
 - ⊕ For this reason, **surrounding an autistic person with things which instill confidence** such as movies, songs, books, podcasts and, in general, positive people, is an excellent hands-off way of helping **autistic** people adapt into our more confident selves. Similarly, guiding **autistic** people away from any material which has the opposite effect can provide the same outcome.
 - **Learn to Accept Failure**


In many examples of confidence-building techniques, people will say that you should look at a misstep as an opportunity to learn and not a failure. However, I am hesitant to believe that there is a lesson in everything, as giving your all, only to come up short, or standing up for


yourself, only to fall flat on your face, is sometimes down to luck of the draw; where subsequently pushing yourself as a result of this misfortune can set false expectations.


This doesn't mean that failure should be avoided at all cost though, in fact, it's quite the opposite, as trying to repress or avoiding any discussion of an awkward incident will only mean that your festering thoughts continue far longer than necessary.

The middle ground here is that, when things do go off plan, **we need to accept that this is just part of life**, where sometimes you win and sometimes you don't. In many cases this is easier said than done, I mean, I still think about when I stuck my hand in Thornton's chocolate fountain and got banned from the shop for life, but being open about it has made me accept it and helped me move on.

- **Take Care of Your Body**


 Okay, so I know you probably saw this one coming (and subsequently winced at the upcoming thought of exercise). However, it really is undeniable that, if you take care of yourself physically e.g. **eating well, working out and getting plenty of sleep**, your **mental health** will improve alongside.


 Of course, this doesn't change the fact that most self-care efforts are long, tedious yawn-fests. Yet, for **autistic** people who can quite easily fall into a rhythm, our minds can give us a head start when it comes to harnessing these advantages; as we are more likely to keep the activities up once we get past the usual hurdles, like restricted eating and general sleep challenge.

 Additionally, thanks to the endorphins which are realized during both eating and exercise, these two activities can help give a temporary boost to self-confidence, which makes them ideal to do before trying out any of the other things on this list (just remember that this is only the case for eating and exercising and not sleeping – as trying to force an **autistic** person to do something the minute we wake up can only spell disaster).

- **Don't Change**

'Fake it 'til you make it', 'Dress for the job you want' 'Play the part', it's frankly bizarre how many times people will say that confidence will come from being something that you are not, when **true confidence comes from being entirely satisfied with who you are**.

 This is dangerous within the **autism** community, where suppressing our identity is so much of a problem it has a name: 'masking'. That's why my last piece of advice today is to simply be yourself.

 Encouraging someone to feel confident in themselves is no easy task though, as it comes from being in the right place, at the right time, with the right mindset and much more. As such, if an **autistic** person does seem to struggle in themselves, try working on external factors that might be standing in the way and not improving the person themselves. For example, maybe harsh lights are making us feel uneasy or maybe too much uncertainty means our mind is somewhere else, for every problem there is a cause and blaming the person and not the problem will only make this a more difficult situation to navigate.

TIPS & STRATEGIES FOR SPECIFIC PLATFORMS

Cellphone (smartphone) security risks

The following has been taken from [Top Mobile Security Threats \(2022\) — Mobile Device Security \(rd.com\)](#)

You might be surprised by the hidden security threats lurking inside your trusty mobile device. Our smartphones are always an arm’s length away, but how many of us are wise to the risks of using them? Mobile security threats are on the rise: Mobile devices now account for more than 60 percent of digital fraud, from phishing attacks to stolen passwords. Using our phones for sensitive business such as banking makes security even more essential. “The more you depend on your phone for everyday tasks, the more it will impact you if your device is compromised,” says Randy Pargman, senior director for Binary Defense, a cybersecurity company. That’s also one of the reasons you should never store certain things on your smartphone.

Luckily, you can still use your phone safely by staying informed and taking precautions. To that end, we rounded up this year’s biggest threats to smartphone security, as well as some expert tips that will help you protect yourself, your phone, and your info.

- **DATA LEAKS**

Before installing a new app on your smartphone, you might want to read the fine print. Nearly every smartphone app collects data from your phone, according to Pargman. That info could include your name, date of birth, credit card and bank account information, location history, contact list, photos, and more. “It’s a little scary when you realize just how much of your activity is collected on servers maintained by the app developers,” Pargman says. If those servers are hacked or if a technical error leaves them vulnerable, all of that data can be stolen and used by criminals for fraud. Pargman suggests adjusting the security controls on your device to limit the data collected by each app and thinking twice before downloading any new app that requests a lot of permissions. FYI, [if these apps are on your phone, someone may be spying on you.](#)

- **OPEN WIFI**

Connecting to [open WiFi](#) networks that do not require a password or use encryption is convenient when you’re in a pinch. But doing so could allow anyone nearby to easily spy on all of your online activity, Pargman says. Even worse, a cybercriminal can create a phony WiFi hotspot in order to trick users to connect to it and steal their data. For example, instead of going to your bank’s website, the WiFi network could direct you to a page that looks just like it and swipe your password when you try to log in. “The safest approach is to only connect to WiFi access points that you know and trust,” Pargman says. “Don’t just connect to anything you find.” If you really have no choice, make sure you [never do these things when using public Wi-Fi.](#)

- **PHISHING ATTACKS**

Cybercriminals often use email, text messages, and even voice calls to fool their targets into giving up a password, clicking on a link to download malware, or confirming a transaction—a practice known as phishing. “Phishing remains one of the most often-used and successful tricks that cybercriminals use to compromise victims,” Pargman says of this mobile security threat. To avoid falling for a phishing scam, always verify who is contacting you for your personal

information. For example, Pargman recommends telling the caller claiming to be your bank that you'll call back using the bank's official phone number. You should also [delete these texts immediately because they are likely scams](#).

- **SPYWARE**

Beware of apps that promise to monitor the activity of your loved ones and children—in reality, they are [spyware](#) that is “designed to allow extremely invasive digital surveillance through a smartphone,” Pargman says. Abusers can use these apps to read texts and emails, track the phone's location, secretly listen to nearby conversations, and take pictures, among other activities. Even less insidious apps can still collect data about what you do on your smartphone, Pargman says. While [making your phone impossible to track](#) can be hard, it's still quite possible to do it to a certain extent to ensure safety. He suggests avoiding apps that request a lot of permissions or any permission having to do with accessibility. “Those permissions give apps the ability to read the text in other apps or control other apps—that's a lot of power that can be abused,” he explains. Watch out for these [red flags someone is spying on your computer](#), too.

- **MALICIOUS APPS**

If you think an app is too good to be true, it probably is, according to Pargman. He calls this the Trojan Horse trick: An app may appear to be beneficial—offering free access to something that should cost money—but it actually contains a virus. “People who take the bait and install these malicious apps are often surprised to find that instead of the promised free material they were hoping for, their entire smartphone is locked, or their data is stolen, and they are faced with threats,” Pargman says. Other times, the virus might secretly transfer money to the attacker's accounts through the phone's online banking app. “The best cure for these malicious apps is prevention,” notes Pargman. Steer clear of apps that promise free access to premium content, aren't listed in well-known app stores, and don't have a history of reviews. These are the [apps security experts would never have on their phone](#).

- **APPS WITH WEAK SECURITY**

Without strong security standards, many smartphone apps can make your information vulnerable to malicious actors. App developers might use weak encryption algorithms that are easy to hack, or unintentionally share digital “tokens” that allow hackers to impersonate real people online. Unfortunately, there is “very little that the average person can do to know which apps don't do a good job with security,” according to Pargman. A good guideline is to be smart about the data you want to entrust to each app, he says. While you may feel comfortable allowing an app to save your email address, you should be more cautious about giving an app permission to access your contacts or store sensitive information such as your Social Security Number or date of birth. You can check out these mobile [security apps](#) to help protect your information.

- **POOR PASSWORD SECURITY**

More than half of Americans reuse passwords across multiple accounts, a 2019 Google/Harris poll found. Those passwords are catnip for cybercriminals, who can gain access to hundreds of accounts by purchasing massive lists of hacked and leaked passwords on the dark web. To protect your accounts from hackers, Pargman suggests setting up multi-factor authentication, as well as using a password manager app to generate and store unique passwords for every

account. “That way, you don’t need to use your pet’s name as your only form of protection to keep your money where it belongs and out of the pockets of thieves,” he says. As you secure your accounts, avoid the [password mistakes hackers hope you make](#).

- **OUT OF DATE DEVICES**

When was the last time you updated your phone? It may be key to protecting your device against malware and other cyberattacks. Phones that are too old to receive security updates should be replaced, according to Pargman. “Even if it seems to still run, there’s risk in using an old phone that hasn’t received the latest security updates,” he says. You can find out how long your device will be updated by checking the “end of life” or “end of support” date on the manufacturer’s website. Samsung updates devices for up to four years, Apple provides regular updates for iPhones for about five to six years, and Google supports its Pixel line of phones for at least three years. FYI, that’s not the only [warning sign it’s time for a new cell phone](#).

- **IDENTIFY THEFT**

Reports of identity theft have sharply increased in the past few years, with millions of cases detected since March 2020 alone. Recently, thieves have used stolen identities to open new mobile phone accounts, or hijack an existing account and upgrade phones or add phone lines. Victims may receive large bills from their carrier or charges from accounts with other carriers that identity thieves opened without the victims’ knowledge. Secure your mobile phone account by creating a password or PIN with your carrier, which will be required to make any changes to your account in the future. Hackers can also do [these scary things with your cellphone number](#).

- **HOW TO SAFEGUARD YOUR DEVICE**

In addition to taking specific precautions for each of the mobile security threats listed above, Pargman recommends downloading anti-virus programs for your smartphone. Apps like Norton Security and Antivirus, McAfee Mobile Security, and Kaspersky Antivirus and Security can help to spot malicious apps if they have been installed. You should also make sure to keep your smartphone’s operating system (Android or iOS) up to date at all times, he says. Here are [more tips to protect your phone from viruses](#).

iPad security risks

The following has been taken from [Top 7 iPad Security Tips \(kaspersky.com\)](#)

Just like your personal computer and smartphone, tablets like the iPad are attractive targets for hackers and identity thieves. In 2017, security professionals discovered the [Broadpwn vulnerability](#) gave cybercriminals the ability to crash Apple and Android devices using Wi-Fi. Preventing someone from accessing your iPad, either remotely or in person, is possible with consistent maintenance and a few changes to settings you can complete in a few minutes. Try these seven strategies for better iPad security.

- **SECURE THE LOCK SCREEN**

If an unauthorized person picks up an iPad with default settings, the notifications visible on the lock screen could reveal personal details about the owner. Snippets of emails, messages from

social media accounts, calendar reminders and more are visible to prying eyes, even if the iPad has a passcode.

Hide sensitive notifications by opening the Notifications menu in the Settings application and selecting the applications that display your information on the lock screen. For example, select the Mail entry to hide the notifications from your email app. The notification settings for different applications vary, but most have an option to hide them from the lock screen.

Strangers may also be able to access the digital assistant Siri or reply to messages without circumventing the lock. *To turn off these capabilities, open the Touch ID & Passcode menu in the Settings application, and select which applications are accessible from the lock screen.*

- **UPDATE AND BACKUP**

One of the easiest ways to secure an iPad is to update the operating system and applications regularly. For iOS updates, the device notifies you when an update is ready, but you can also check manually in the Settings application. Open the App Store to check for application updates, which are essential for security purposes, even for seldom-used applications.

Before installing an iOS update, update your iPad's backup in iTunes or iCloud to ensure you can recover from any issues that could arise during the installation process. For maximum security, you can encrypt these backups in just a few easy steps. A recent backup is the best defense against ransomware and other cyberattacks.

- **SECURITY BROWSERS**

You may automatically use your iPad's native Safari browser, but is it keeping your data secure on the web? Safari's Private Browsing mode ensures a web page in one tab can't see pages open in other tabs. It also prevents any new website data being stored on your device, and it automatically asks websites not to track your browsing.

If you require even stronger security, some third-party browsers provide more control over security options and offer privacy-focused versions of their normal browsers. Before downloading any new applications, find the application publisher's official website, and follow a link from there to the App Store to ensure you download a legitimate version.

- **MANAGE APPLICATION PERMISSIONS**

Not paying attention to application permissions means an application could access your location, microphone or contacts without your knowledge. Look for application permissions in two different places in iOS. Most are in the Settings application under the particular application's name. From that menu, select specific permissions to allow and reject. Others are managed under the Privacy menu in the Settings application. Choose a permission heading, such as Microphone, to see all the applications that have that permission. This is an easy way to ensure no application has access to Health data, Calendar events or other items that you would prefer to keep private.

- **MAKE SURE “FIND MY IPHONE” WILL WORK**

A thief who takes your iPad could turn off Find My iPhone's access to the device's location, negating the advantage of having an app that allows you to geolocate your device from another device. Even if the thief figures out your primary passcode, setting an application permission restriction prevents him or her from blocking Find My iPhone. This change is under the General menu in the Settings application. Choose the Restrictions option, decide on a unique passcode and then turn off the ability to allow permission changes for Locations and Accounts.

Restrictions are also a good way to ensure your child cannot access your Apple Wallet to make in-app purchases while playing a game or change other settings that could compromise his or her safety.

- **CHOOSE A MORE SECURE PASSCODE**

In some versions of iOS, the default passcode is only four digits long. This is relatively easy for a sophisticated cybercriminal to crack. Navigate to your Touch ID & Passcode menu, and choose the option for changing your passcode. Disable Simple Passcode, and enable Custom Numeric Code or Custom Alphanumeric Code to create a longer passcode that is more secure. You can also decide whether you want your iPad to wipe itself after a certain number of unsuccessful access attempts.

- **ADVANCED OPTIONS**

If you want to manage multiple iPads in a family or fine tune a personal security policy, Apple provides a tool for that. Apple Configurator 2 gives you the ability to design a policy for iPhone and iPad security on one computer and then share it with all relevant devices. This is a good solution if you need to secure devices used by less security-savvy people, such as children.

Regardless of your own familiarity with iPad security, it's important to take the right steps to keep your device secure. Install a strong mobile security program, and follow these useful tips.

Mac security risks

The following has been taken from [Mac Security & Privacy \(kaspersky.com\)](#)

MacBooks come with a variety of built-in security settings, but they are not always used to their full advantage. This can leave your data and privacy vulnerable to cybercriminals. While it's not possible to totally lock down and secure your computer, you can maximize your Mac's security and privacy and protect yourself from cyber threats by going through your settings and establishing a good set of defenses. Read on to find out how.

- **DON'T TURN OFF AUTOMATIC UPDATES**

It's important to keep your apps and Mac operating system up-to-date because security updates address software vulnerabilities. If you don't keep updated, [hackers could exploit vulnerabilities](#) to gain access to your data. Modern Macs have automatic updates enabled by default – it's worth checking that your computer is properly downloading them.

To make sure software updates are running correctly:

- *Open System Preferences then Software Update*

- *Click the Advanced button*
- *Be sure to check all the boxes*
- *These updates may require you to restart your computer*

To make sure app updates are running correctly:

- *Within System Preferences, click on App Store and then enable automatic updates*

- **ENABLE FILEVAULT**

FileVault is software for encrypting your device. It jumbles up your device's data so that it's incomprehensible to anyone without your password. This means if you lose your device or it's stolen, nobody else will be able to access anything on your storage drive. On more recent Macs, FileVault is probably enabled by default. But if you have an older Mac, or you opted out of the feature when you set up your Mac originally, you should check to see if it's turned on.

To do this:

- *Open System Preferences, click Security & Privacy and select the FileVault tab*
- *Click Turn On FileVault and follow the on-screen instructions*

Apple gives you the option to store your recovery key in your Apple account or locally. For most people, if you have a [strong password](#) for your Apple account, you're better off storing the recovery key there. But if you're not comfortable with that, or if you store a lot of very personal data on your device, you can opt to store the code yourself. If you choose to do so, it's important that you don't lose the key or forget the password you create, as you won't be able to access your data if you lose either one.

- **PASSWORD PROTECT FOLDERS**

Knowing how to password protect a folder on Macs is useful. This feature allows you to store sensitive information and ensure that only somebody with the password can access it. You can do this without installing any extra software by using your Mac's Disk Utility app. It doesn't password protect the folder itself. Instead, it creates a separate folder disk image, but the effect is the same. You can open the folder disk image and move files in and out as normal. It's possible to share the folder disk image with other people and, provided they know the password, they can access files in the folder as well.

To password protect a folder on Mac:

- *Open the Disk Utility app. You can do this by launching Finder, clicking Applications in the left-side menu, and then clicking the Utilities folder.*
- *You can also find it via Spotlight – press the Command and Spacebar on your keyboard and type Disk Utility.*
- *With Disk Utility open, click File and move your mouse over New Image.*
- *Click Image From Folder from the list of options.*
- *Select the folder that you want to password protect and click Choose.*
- *You will need to choose a level of encryption. Click the Encryption drop-down and select either 128-bit AES encryption or 256-bit AES encryption.*
- *Your choice will depend on what you're looking to password protect. If the information is very sensitive, choose 256-bit AES encryption because it offers a higher level of*

protection. For speed and efficiency, however, 128-bit AES encryption is more than sufficient.

- *Now enter the password you want to use to protect the folder. Enter it again to verify.*
- *Click the drop down box next to Image Format and select read/write – this will ensure you can edit your folder in the future. Click Save.*
- *A folder disk image will be created (it will have the suffix .dmg). It may take some time. When it's complete, click Done.*
- *You will now have two folders – the disk image and the original folder. The original folder will be unprotected. If you don't need the non-password protected folder, remember to delete it.*

- **ENABLE THE BUILT-IN FIREWALL**

Apple has a built-in firewall that helps to block unwanted inbound network connections and keep malware out of your network and device. This provides a useful layer of protection but it is turned off by default, so you need to manually turn it on to benefit from it. To do this:

- *Go to System Preference then open Security & Privacy*
- *Click on the Firewall tab*
- *Click on Turn On Firewall*

For more advanced users, you can review Firewall Options to select more detailed settings. Otherwise, you can simply let the default settings apply. Bear in mind that Apple's firewall guards against incoming traffic only and does not prevent data from being sent out. For additional security, you can consider using a third-party firewall which offers more advanced protection.

- **BACK UP YOUR FILES**

By regularly backing up your files, you ensure you always have copies if something happens to your Mac – for example, if it's lost, stolen or needs to be repaired.

You can use Apple's Time Machine feature to back up your files. Time Machine backs up files on a separate, external hard drive which allows you to restore your Mac and data from a specific recent time.

To set it up:

- *Connect an external hard drive that is the same size or bigger than your Mac's drive and has no other files stored on it*
- *Open the Time Machine app from System Preferences*
- *Click Select Backup Disk, select the name of your disk, then click Use Disk*
- *By ticking Back Up Automatically, you won't have to remember to backup manually*

Once set up, Time Machine works automatically, provided your external drive is connected to your Mac. It will send you reminder notifications if you don't connect your external drive for a while. If your external disk runs out of space, Time Machine automatically erases the oldest versions of the files to make room for new ones.

- **CONSIDER A GUEST ACCOUNT FOR OCCASIONAL VISITORS**

If you have occasional visitors, rather than giving them a full account of their own, use the Guest account available at the login screen. This will enable them to use apps and the internet but

won't allow them to see files you have stored on your Mac. MacOS creates a temporary workspace and deletes it when the guest logs off.

If your Mac is lost or stolen, and you have set up iCloud's Find My Mac option, when a guest logs on and connects to the internet using Safari, Apple can track your Mac's location.

- **DELETE SOFTWARE YOU DON'T NEED**

Depending on how long you have owned your Mac, you may have software on it that you no longer use. Unused software takes up space on the drive but, more critically, can sometimes create a security risk, as it may contain vulnerabilities that remain exposed. Apple allows users to check for old or unused apps on their Mac.

To do this:

- *Click on the Apple icon in the top right corner of your screen*
- *Select About This Mac*
- *Click on the Storage tab, and then click Manage*
- *Click on Documents and then choose Unsupported Apps to see a list of programs your Mac no longer supports — then delete them all*
- *Then click on Applications and sort by 'Last Accessed' to see apps you have not used in a long time, which you may want to delete*

- **REVIEW YOUR MAC PRIVACY SETTINGS**

As with your phone, your Mac has various privacy permissions as over time, you have granted or denied apps access to different types of information such as your location, contact or calendars. It's good practice to review these permissions regularly to make sure they are set to a level you remain comfortable with.

To do this:

- *Open System Preferences and going to Security & Privacy*
- *Select the Privacy tab*
- *Go through each permission and uncheck any that feel unnecessary (you can always reinstate permissions later if you change your mind)*

Generally, if you're in doubt about whether an app needs permission or not, it's best to be cautious by restricting access.

To check if you are unknowingly sending usage data to Apple and other app developers, click Analytics & Improvements at the bottom of the left-hand menu. Then uncheck the options for data you don't want to be sent automatically to Apple or other app developers.

- **REVIEW SAFARI PRIVACY SETTINGS**

If you use Safari on your Mac, it's worth reviewing Safari's privacy settings.

Some useful shortcuts to know include:

- *New Private Window (Shift + command + N): This enables private browsing, allowing you to browse the web without recording your visits in the History menu*
- *Clear History in the Safari menu: This erases cookies and other cached data in the History menu*

- *Privacy section in Safari's Preferences: This helps to prevent websites from tracking you or storing cookies on your computer*

- **SET UP FIND MY MAC**

The Find My Mac feature is useful in case your Mac is lost or stolen. Not only will this tool help you find your Mac, but it will also enable you to wipe your drive remotely if your device is lost or stolen.

To set it up:

- *First turn on Location Services in your privacy settings and select Find My Mac in the list of apps that can use your location*
- *Then, click on the Apple menu icon and select System Preferences followed by Security & Privacy then Location Services*
- *Click the padlock and enter your password*
- *Select Enable Location Services and select Find My Mac and lock the padlock to prevent further changes*

- **SET UP A STRONG COMPUTER PASSCODE AND ENABLE TOUCH ID IF YOU CAN**

When you leave your computer unattended, it's a good idea to have a screen saver that can only be turned off with a password. You should set up a screen saver that will start after your computer has been idle for a set interval.

To set your computer to lock your screen automatically:

- *From the Apple menu, choose **System Preferences***
- *Click **Desktop & Screen Saver***
- *Click **Screen Saver**, and then use the slider to choose **15 minutes** (or less)*
- *Click **Show All** to go back to the main System Preferences window*
- *Click **Security**, and then click **Require password to wake this computer from sleep or screen saver***
- *Close the System Preferences window*

If you have a more recent Mac, you might be able to log in with Touch ID. If you didn't enable that feature when setting up your computer, you should do so now. It makes logging in quicker and easier and gives you scope to create a more complicated password since you don't have to type it so frequently.

To set up Touch ID:

- *Open System Preferences, then Touch ID*
- *Select Add A Fingerprint and follow the on-screen directions*

Your computer's password still serves as a backup login option and will be required whenever you restart your machine, but you can make it as long as you wish since you won't have to type it so often. The longer your password, the more secure it is likely to be. Touch ID support also extends to some apps, which makes unlocking them less of a chore.

- **LIMIT APP PURCHASES TO THE APP STORE**

To minimize your risk of [malware](#) and harmful apps, only use apps from a known and trusted source like the App Store. Never download unlicensed or pirated apps from the internet.

Harmful apps can often be disguised as a movie or graphics file. These apps, called [Trojans](#), are often spread by internet downloads and email attachments. If you see a warning that a file you receive is an app – for example, a file sent to you in an email – don't open it and delete it from your Mac.

It's also a good idea to read trusted reviews of apps before downloading them. This may help you avoid malicious apps and ensure you're downloading a legitimate app onto your device.

- **BE CAUTIOUS WHEN GRANTING APP PERMISSIONS**

If you give apps access to your Mac, you also give them access to your contact, calendar, and other information, and are subject to their terms and privacy policies and not the Apple Privacy Policy. Before you download an app, review its terms and privacy policy to understand how it treats and uses your information. Only grant access to apps that you know and trust.

- **BE WARY OF PHISHING SCAMS AND POP-UPS**

One of the best ways to protect yourself online is by learning how to spot online scams. This includes recognizing [phishing](#) attempts and being careful about what you download.

To avoid falling victim to phishing, never click on links in text messages, emails, social media messages or any message which looks suspicious. These could be messages designed to trick you into disclosing personal information such as credit card numbers or passwords.

If you do receive an email claiming to be from your bank asking you to verify login information, look closely at the sender's details to check who it is from. When in doubt, go directly to your bank's site in your web browser and avoid clicking on any link within the email. To test your ability to recognize phishing scams, you could try Google's [Phishing Quiz](#).

- **ENABLE 2FA ON YOUR ICLOUD ACCOUNT**

Two-factor authentication or 2FA involves inputting a randomly generated one-time code along with your password when logging into your accounts. This provides an additional layer of security because, even if hackers know or guess your password, they won't be able to guess the randomly-generated code. This prevents them from accessing your accounts.

To set up 2FA on your iCloud account:

- *Go to System Preferences then Apple ID then Password & Security*
- *Then go to Two-Factor Authentication and click Turn On*
- *You will then be asked to input your phone number to receive the two-factor authentication codes*

Once set up, you will receive a one-time password each time you log into your iCloud account on a new device or when logging in online.

- **CONSIDER USING AN AUTHENTICATOR APP**

You can take 2FA a step further by using an authenticator app. An authenticator app generates unique codes on the spot, rather than sending them via SMS text message, which cybercriminals could intercept. Some password managers also offer this feature.

- **USE A PHYSICAL SECURITY KEY**

Another method of implementing 2FA is by using a physical security key or token. This is like a smart card that provides your digital signature and is an option for users who want additional protection. No one can access your Mac without presenting your security key or token, even if they know your password.

- **USE A VPN**

A [VPN or Virtual Private Network](#) disguises your original IP address and replaces it with an [IP address](#) in a different location. This means that hackers and websites can't trace your connection, increasing your anonymity online. VPNs also encrypt your browsing data, which means that hackers can't see what you're doing. VPNs are used for a variety of purposes, but online privacy is chief amongst them. There are various VPNs on the market, including [Kaspersky Secure Connection](#).

- **DISABLE REMOTE ACCESS AND SHARING**

Remote access can be useful if you need to access your Mac from anywhere. However, if your login details are compromised, this means others could also be able to remotely access all your files and data. So, it's a good idea to disable this feature when you don't need to use it.

To do this:

- *Go to System Preferences then Sharing*
- *Untick the boxes next to Remote Login, Remote Management, and all the other sharing services you don't need*

- **USE A PASSWORD MANAGER**

It's essential to use a secure password to lock your Mac. **Using unique, complex passwords for all your accounts is essential in today's online environment.** But, with the hundreds of online accounts we now need for our day-to-day activities, remembering so many unique passwords is very difficult, if not impossible. While some users are tempted to use the same password for everything, this can be a mistake; if your password is hacked, your entire online identity is compromised. Using a [password manager](#) is a great solution.

Apple offers its own password manager called iCloud Keychain. This works by saving and securely storing your account login credentials, passwords, and payment card information. All information is encrypted with AES 256-bit encryption, considered military-grade encryption. While iCloud Keychain can be useful, it is limited in that it can only be used for Apple products, so if you also have an Android phone and a Windows PC, you won't be able to sync your passwords between devices. For this reason, many users decide to use a third-party password manager that works with all operating systems and can seamlessly sync between devices.

- **TURN OFF WI-FI AND BLUETOOTH WHEN YOU DON'T NEED THEM**

If you aren't using Bluetooth — or if you are in an environment you don't trust — then it's good practice to turn it off. This reduces your Mac's discoverability and adds an extra layer of privacy. It can help prevent any potentially dangerous connections.

To turn off Bluetooth:

- *Select the Apple menu icon then System Preferences then Network then Bluetooth then toggle Bluetooth to Off*

- **TURN OFF SIRI**

Siri is your Mac’s intelligent personal assistant. It can share personal information, so some users prefer to turn it off when not in use.

To turn off Siri:

- *Select the Apple menu icon then System Preferences then Siri then toggle on or off Enable Ask Siri*

- **CONSIDER ENABLING LOCKDOWN MODE**

[Included within iOS 16](#), Apple’s Lockdown Mode helps to protect devices against rare and extremely sophisticated cyber attacks. Apple considers it an extreme protection that’s designed for the very few individuals who, because of who they are or what they do, could be personally targeted by some of the most advanced digital threats – for example, from hostile nation states. Most users won’t be subject to these kinds of threats.

Apple states that when Lockdown Mode is enabled, your device won’t function like it usually would. To reduce the attack surface that could potentially be exploited by highly targeted mercenary spyware, certain apps, websites, and features will be limited for security, and some experiences may not be available at all. For example, Lockdown Mode blocks link previews in the Messages app, turns off potentially hackable web browsing technologies, and prevents incoming FaceTime calls from unknown numbers.

Most users don’t need Lockdown Mode but if you do want to turn it on, here are the steps to follow:

- *On your device, open Settings*
- *Navigate to Privacy & Security*
- *Scroll to the bottom and select Lockdown Mode*
- *Select Turn On Lockdown Mode*

- **ENABLE FIRMWARE PASSWORD**

If you have an Intel Mac, you can use a firmware password to prevent people from using alternative startup disks and removable media to boot your Mac without authorization. A firmware password significantly improves security for those who share devices and works as a strong anti-theft measure.

To turn on a firmware password:

- *Start up from macOS Recovery*
- *When the utilities window appears, click Utilities in the menu bar, then choose Startup Security Utility or Firmware Password Utility*
- *Click Turn On Firmware Password*
- *Enter a firmware password in the field provided then click Set Password*
- *Quit the utility, then choose Apple menu then Restart*

Your Mac asks for the firmware password only when attempting to start up from a storage device other than the one selected in Startup Disk preferences, or when starting up from macOS Recovery. Enter the firmware password when you see the lock and password field.

- **USE A GOOD QUALITY ANTIVIRUS FOR MACS**

It's always a good idea to use a comprehensive and up-to-date antivirus. Whilst macOS comes with XProtect anti-malware protection and other safeguards, you can gain additional protection by using a complete antivirus for Macs.

Protection on social networks

The following has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)

12 WAYS TO IMPROVE SOCIAL MEDIA AND ONLINE COMMUNICATION



There are a lot of benefits to using social media, especially for people with **autism** 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:

- **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.
- **Never comment about your work 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.
- **Refrain from posting content that might skew other people's opinions 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.
- **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.
- **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.
- **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.
- **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.
- **Always be polite in your online discourse and avoid arguments**, even when you feel that the other person is wrong.
- 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.

- 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.
- **If someone is making you feel uncomfortable or unsafe, leave the situation** and block them.
- **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.

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.

The following has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#), [How to Filter, Block, and Report Harmful Content on Social Media | RAINN](#), [Twitter Age Limit: Is My Child Safe? \(natterhub.com\)](#), [Twitter has FINALLY released this risk management feature \(aleciahancock.com\)](#) and [15 Twitter Safety Tips to Protect Your Account and Identity \(makeuseof.com\)](#)

-- TWITTER --

What are some of the main risks of Twitter?

- A **troll** is someone who deliberately starts arguments by intentionally making rude or upsetting comments to encourage strong emotions in others or to steer the conversation off topic. This act is common on Twitter. Trolling can lead to devastating consequences for its victims.
- Twitter is a very public site where users are encouraged to tweet about anything they like. **Inappropriate language and swearing** is allowed if it doesn't violate the rules.
- Twitter has been associated with **fake profiles and fake news** too. Both of which could be easily used to scam or take advantage of vulnerable individuals.
- The use of **hashtags** originated with Twitter. If used properly they can be used to search for particular interests. They can also be misused with some users hashtagging under a particular hashtag with different intentions, exposing people to inappropriate content.
- 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:

- **Never share personal information.**
This has to be the first and foremost guideline and cannot be stressed enough. Never share your email, personal or business address, telephone numbers, and other private information on

Twitter publicly. Doing so puts you at risk of identity theft. You should only share personal information via private message when you are absolutely sure of who you are talking to.

- **Turn off geotagging on your tweets**

Make sure you also disable geotagging on Twitter. It is an optional Twitter feature that makes your location public on your tweets.

To turn off geotagging, open Twitter's settings and head to Privacy and Safety > Your Tweets > Add location information to your tweets, then make sure the checkbox is not ticked.

- **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 from 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.

Regularly review which applications can access your account

- **Avoid web-based applications** that ask you to supply your Twitter username and password. Well-behaved applications use Twitter OAuth and do not ask you to provide your Twitter password.
- **Regularly review the list of applications** you have authorized to access your Twitter account by following the steps below:
 - Open Twitter's settings.*
 - Click on Security and Account Access.*
 - Select Apps and Sessions.*
 - Click on Connected Apps.*
 - Remove all applications from that list that you no longer need or use by clicking on the app's name and select Revoke Access.*
- **Unmention yourself**
If you choose to unmention yourself, your username will be untagged in original tweets and replies, users won't be able to mention you again in the same reply chain and you won't get further notifications.
- **Change your password frequently**
Automated bots can be used by hackers to gain access to your Twitter account. So use strong passwords and keep changing your password every six weeks to ensure maximum safety.
 - To make sure your password is safe, you can use a free password generator website and enter the various parameters you require.*
 - To change your Twitter password, go to Settings > Your Account > Change your password.*
- **Preview short URLs before you click**
Shortened URLs are often used to hide unsafe web addresses. Visiting unsafe websites carries the risk of malware, phishing scams, and identity theft.

By default, Twitter will add a site preview when a link is inserted into a tweet. However, the creator of the tweet can remove the preview before they publish it.

If there is no visible preview, paste the link into a tool like [TrendMicro's Site Safety Center](#) to check its safety before you click.
- **Beware of unsolicited DMs (direct messages)**
Phishing attacks often use targeted private messages to lure unsuspecting users to a login page where they are asked to provide their username and password.

The problem is that you may receive a direct message from a trustworthy user you are following whose account has been compromised. After all, there is no foolproof way to ascertain whether a message is authentic or suspicious.

You should use your judgment and discretion while clicking URLs in direct messages. If there is any reason to suspect that the message is strange in any way, simply delete it and let the user know.

- **Consider making your account private**

If you are using Twitter to communicate among a chosen group of friends, colleagues, or family; consider making your Twitter feed private. This step is also recommended for youngsters on Twitter.

To make your Twitter account private, follow the steps below:

Open Twitter's settings.

Select Privacy and Safety.

In the Your Twitter activity section, click on Audience and tagging.

Mark the checkbox next to Protect your tweets.

By selecting this option, your account information and tweets you have sent will only be visible to people who follow you.

- **Block and report spam**

If you receive lots of spam, block and report the account. Many Twitter clients let you do that from within their interface and you can also do it from within Twitter's main web app.

Reporting a tweet is easy. Click on the three horizontal dots next to the tweet and select Report tweet. You will need to choose your reason for the report before you submit it. The available options are I'm not interested in this tweet, It's suspicious or spam, It's abusive or harmful, or It expresses intentions of self-harm or suicide.

For spam, you need to choose the second option and then select one of the following choices:

The account tweeting this is fake.

Includes a link to a potentially harmful, malicious, or phishing site.

The hashtags included seem unrelated.

Uses the reply function to spam.

It's something else.

In a few days, Twitter will let you know how it has dealt with your report.

- **Don't buy followers**

It's tempting to use one of the many services that offer followers for sale or that promise to get you "hundreds of followers quickly".

Not only are such services a guaranteed way to make your Twitter account suspicious and lead to your account being suspended, but Twitter frequently deletes millions of accounts that sellers use to fulfill orders. The followers you buy, therefore, don't tend to stick around for long.

- **Report an account for impersonation**

Twitter only permits impersonation for parody. Yet even if you don't use Twitter at all, someone else may be using your name to impersonate you on Twitter. This can lead to grave reputation problems for your business interests, professional life, and personal life. If you come across any Twitter account impersonating you in an illegitimate fashion, you can report the user directly from the Twitter app.

Just open the profile, click on the three horizontal dots, select Report [user], and choose They're pretending to be me or someone else.

If you are not a Twitter user, use [Twitter's standalone impersonation report form](#) instead.

-- FACEBOOK --

What are some of the main risks of 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**

Log in 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 from 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.

-- INSTAGRAM --

Ways to protect yourself on 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.

- **Block comments from specific individuals:**

This will hide the comments of a blocked individual from your posts. The blocked individual will be the only one able to see their own comments.

Go to your profile and select the menu button (3 horizontal lines) > Click Settings > Privacy > Comments > Select “Block Comments From” and enter the username of any users that you do not want to comment on your posts or stories.

- **Hide generally offensive comments:**

This will hide comments on posts, stories, and live videos which Instagram deems to be inappropriate or offensive.

Go to your profile and select the menu button (3 horizontal lines) > Click Settings > Privacy > Comments > Use the toggle to turn on “Hide Offensive Comments.”

- **Restrict an account:**

Restricting an account will protect you from unwanted interactions without having to block or unfollow the individual. This setting will make it so only you and the individual can see their

comments on your posts. They will also be unable to see when you're online or when you have read their messages. The individual will not know if you have restricted them.

- **Through settings:** Click *Settings > Privacy > "Restricted Accounts."*
 - **Through comments:** *Swipe left on a comment from the individual you want to restrict > Click the Exclamation Point Button > Select "Restrict."*
 - **Through their profile:** *Click the menu button (...) in the top right corner of their profile > Select "Restrict."*
- **Filter specific words or phrases:**
This will hide comments that contain any of the specific words or phrases you have chosen to filter out.

Go to your profile and select the menu button (3 horizontal lines) > Click Settings > Privacy > Comments > Use the toggle to turn on "Manual Filter" > Enter any words or phrases that you do not want to see, separating words and phrases with a comma.

You may also select "Filter Most Reported Words," which will hide comments that contain words which have been commonly reported on your posts and stories.

- **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.

-- SNAPCHAT --

The following has been taken from [Cyber Safety Tips and Tools — PAAutism.org, an ASERT Autism Resource Guide, 2022 Snapchat Scams: Don't Fall For These 7 Devious Tricks | Aura](#)

Ways to protect yourself on Snapchat:

- **Restrict who can contact you:**
By default, only friends you've added on Snapchat can contact you directly or view your story.

To change that, go to the settings from your profile screen and choose the "Who Can..." section. Here you can change who can contact you, view your story or see you in Quick Add.

- **Separate real from a fake Snapchat account:**
 - **Check their Snap score.** This will show if they’re actively using the platform. If they claim to be an influencer and have a Snap score of just a few hundred, it’s likely a scam.
 - **Look at the Snap map.** Does their real-life location match what they say in their profile?
 - **Search their profile/story photos in Google image search.** Scammers will steal images from other sites and use them for their fake accounts. Upload a photo to Google image search to see where it came from.
 - Go to [Google Images](#) and click on the camera icon beside the search bar.*
- **Check if they have a Bitmoji.** A Bitmoji is the cartoon avatar by a person’s name. Because it’s so common for Snapchat users to have these, it can be a red flag if an account isn’t using one.
- **Think about what they’re asking you.** If a random account adds you and starts asking for “help” or sending you strange links, you should probably block them. This also goes for your friends. If someone you know starts sending you strange messages, contact them on a different platform and ask if everything’s OK.

Fake accounts often feature attractive models and people flaunting cash, luxury goods, and sports cars. But never forget the golden rule of [fraud prevention](#): “If it seems too good to be true, it probably is.”

Protection on gaming sites

The following has been taken from [Video game security: Online gaming safety tips | Norton](#), [Online Gaming - The Risks Parents Need to Know | Internet Matters](#), and [Video game security: Online gaming safety tips | Norton](#)

Whether you’re a professional gamer, a casual player, or the parent of a child glued to their PC, if you don’t have an eye on video game security and lack protection for your devices, you risk a number of serious risks.

The unfortunate fact is there are many ways hackers can access your information while playing online, and even more ways they can turn that information into profit. With the proper protection — along with online gaming safety tips — you can stop hackers in their tracks before they become a problem. But, first, you have to know what you’re up against.

COMMON VIDEO GAME ATTACKS AND RISKS

→ **Addiction**

There has been a lot in the news about online gaming addiction as one of the risk factors associated with video games. This is not surprising. As with any hobby — football, chess, reading — those who enjoy playing video games for leisure will do so enthusiastically and deeply. This can lead to a desire to play for longer and more frequently. Of course, video games are designed to minimize the hurdles to repeat play and maximize enjoyment. This persuasive approach means it’s important to utilize screen time limits (available on consoles and smartphones) as individuals develop their own healthy boundaries.

→ **Infection**

The oldest trick in the book is still one of the most effective — and infective. When gamers try to find a cheaper or free version of their favorite games available for download, they

risk downloading malware and viruses instead. This threat isn't solely from illegally downloaded games. Cheat codes, items bought through third-party sellers, and even the occasional security gap in games we download legally could pose a risk.

→ **Account takeover**

Sure, it's much easier to use the same username and password for all of your favorite gaming platforms, but that also means it's a breeze for hackers to gain access to all of your accounts. In fact, hackers probably count on you not being able to remember multiple log-ins, giving them the ultimate upper hand.

→ **Swatting and doxxing**

After cybercriminals find your personal information, they could publish your home address and phone number online or send law enforcement to your home by reporting a fake emergency. Not only is this scary, but it's dangerous. This is a hacker's way of saying they know where you live and how to find you.

→ **Active listening**


When you're having a conversation, active listening is a good thing. But when you accidentally leave your mic, camera, or screen capture on and mention or show any personal information, you may be at risk of a swat attack, dox attack, or your bank account being hacked.


• **Cyberbullying**

Players who purposely harass and provoke other players (called *griefers*) in order to spoil their enjoyment — thrive in an online environment. Having the ability to hide behind avatars and characters makes it easy to create an alter ego who thrives off aggravating others.

- *Solution:* Cyberbullies use online social videogames to find and harass their victims. In order to get rid of them, try taking a screenshot of the bullying. Make sure their username is visible and report them to the video game's admins. You can also try blocking the bully to prevent them from interacting with your character online.


• **Privacy/ Players who pray on overshapers**


 **The language in this section has been changed from "children" to "vulnerable populations (such as children or those with ID/D, autism or disabilities)"*

 Vulnerable populations (such as children or those with **ID/D, autism or disabilities**) can be natural overshapers. For those people's perspectives, it makes sense to share everything about themselves because that's how friends are made. However, by using normal friend-making tactics with strangers online — such as telling other players where they live, how old they are, where they go to school, or using identifying information in their usernames and passwords — they may risk putting themselves and their families in danger.

- *Solution:* Remind them not to share personal or identifying information with strangers online. Even though they play together, they don't truly know that person or their intentions. Sit down with them and go over their account's privacy settings to make sure they **stay safe while gaming**.


• **Predators**

 **The language in this section has been changed from "children" to "vulnerable populations (such as children or those with ID/D, autism or disabilities)"*


 Predators may create gaming accounts specifically to befriend vulnerable populations (such as children or those with **ID/D, autism or disabilities**) through online gameplay. After gaining their friendship, they might lure them into meeting up offline.

- *Solution:* Research which of the person’s favorite games include social features such as chat boxes and mic options. This way you’ll know when to closely monitor the in-game interactions and report any suspicious activity.

- **In-game purchases/ Using parent’s bank accounts**


 **The language in this section has been changed from “children” to “vulnerable populations (such as children or those with ID/D, autism or disabilities)”*

**The language in this section has been changed from “parents” or “mom and dad” to “parents or guardians”*

 Possibly the most common video game threat for vulnerable populations (such as children or those with **ID/D, autism or disabilities**) is one that mostly affects their parent or guardian’s bank accounts. Some individuals might use their parent or guardians credit card to make in-game purchases without their knowledge. And due to the existence of friendly fraud — when consumers make a purchase and then request a chargeback from their bank — it can be extremely difficult for parents to get their money back.

- *Solution:* If the individual needs your credit card for making an account or purchasing something online, make sure you’re the one inputting the card information. This way, if there is an option suggesting using this card information for all in-game purchases, you can make sure the box is unchecked. It might also be a good idea to enable password protected purchases wherever possible.

Understanding parental controls on gaming sites

 **The language in this section has been changed from “children” to “vulnerable populations (such as children or those with ID/D, autism or disabilities)”*

**The language in this section has been changed from “parents” or “mom and dad” to “parents or guardians”*

The following has been taken from [Video game security: Online gaming safety tips | Norton](#)

These online gaming safety tips could help boost video game security.

- **Use strong, unique passwords**

One of the easiest ways to help protect yourself is by making sure your **passwords** are different across all platforms. If you want to go the extra mile, then you can even update your passwords once every month so that nothing stays stagnant. When creating your password, make sure you use a combination of upper and lowercase letters as well as numbers and symbols to make it as strong as possible. A long passphrase that only you would know is another option. You might even want to look into using two-factor authentication so that you’re the only person who can access your accounts.

- **Don’t share personal information**

From using your real name or where you’re from in your username — not good — to saying your personal information out loud through your headset, there are many ways you can accidentally let something slip while playing video games online. It’s best to make sure there are no identifying factors on display in your username and that you don’t share any personal details on

gaming forums. You can even use a [VPN](#) to disguise your IP address to stop hackers from trying to gain access to your console or PC.

- **Only download from reputable sources**
Third-party add-ons, illegal downloads, and cheat codes may seem like a good idea at the start, but the consequences outweigh the promised benefits. Keep your computer and yourself safe by avoiding third-party systems and ditching illegally downloaded video games.
- **Use up-to-date, secure equipment**
Keep your worries to a minimum by downloading security software specifically designed to keep gamers safe. Make sure to update your devices and the software regularly in order to keep everything up to date and running smoothly.
- **Avoid opening suspicious links**
 - The gamer may see a link that a player has provided in in-game chat. Best advice: Don't open it. Phishing and other link-based scams are all too common, and you never know who's sending a link, or where it points, until it's too late. Remind the gamer that the link is coming from a stranger. Opening the link could compromise your account. It could also put malicious software on your device, steal your credentials, and put your information and gaming assets up for sale.
- **Never share account information**
 - It's important to explain to the gamer why they should never share account information. Their account may contain valuable personal information and digital data. Plus, it may be tied to a credit card account. They should also understand that there are types of information that game companies would never ask for — like bank account numbers or Social Security numbers. Don't ever give this information out.
- **Be careful with microtransactions and community markets**
 - To take advantage of the growing gaming market, developers frequently release new in-game items, map packs, and updates available for purchase in their store. The gamer will probably want to buy certain virtual goods. After all, the goods can enhance a game character or improve the gaming experience. Some games have markets allowing players to buy, sell, and **trade in-game content**. If the gamer is going to participate, here's some advice: Only use legitimate markets on the game brand's platform.

Protection on online dating sites

The following has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™, sarrc-online-safety-manual_3-e.pdf \(nextforautism.org\)](#)

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 café, 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.

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.

HOW TO IDENTIFY SAFE AND UNSAFE DATING WEBSITES

Learn about who visits the site/app and what they are looking for: Some are targeted for people looking for casual relationships or sexual encounters

IMPORTANT CONSIDERATIONS WHEN PAYING FOR DATING SITES

Ensure secure site; understand how they protect your information by reviewing privacy policy

Do not sign up for auto withdrawal from an account; ensure you are able to cancel at anytime

Make sure you are getting something of value for the cost; review all the terms and conditions before signing up

TIPS & STRATEGIES FOR SPECIFIC RISKS

Digital & sensory overload


The following has been taken from [What Is Digital Overload, and How Does It Affect Our Health? – GoodRx](#)

Digital overload is when using tech devices like smartphones, computers, or TV exposes you to more sensory information that you can process. It can result from habits such as spending too much time on devices, consuming too much information and multitasking with different media. Sensory overload occurs when one or more of the body's senses experience over-stimulation from the environment. For those who experience sensory sensitivity, electronic devices and the internet can trigger an all-round overload.

HOW MUCH DIGITAL CONSUMPTION IS TOO MUCH?

- Research has not quite figured out what our limit is when it comes to time online. However, experts recommend less than 2 hours of screen time per day for most children under age 18. For children under age 5, pediatricians recommend even less screen time.
- It is likely that for adults, too, it's better to limit time spent on devices. Generally, adults should aim for less than 2 hours of screen time a day outside of work. This can help you avoid the problems associated with spending too much time online.

SIGNS YOU MAY BE EXPERIENCING DIGITAL OVERLOAD

 Loud noises, bright backlights, unexpected music, and auto-playing videos are just a handful of the irritants that can overwhelm. For **autistic** people who can be more sensitive to this kind of stimulation, computer use can exacerbate a number of different triggers and symptoms. Some signs that someone might be experiencing digital overload include:

- Irritability
- Anxiety and or depression symptoms
- Difficulty sleeping
- Mood swings
- Physical symptoms (e.g., headache, visual problems, issues with sleeping, high blood pressure, etc.)
- Spending less time with family
- Decrease in other activities that you used to enjoy
- Potential issues being caused at work as a result of being on your device

STRATEGIES TO LOWER RISK FOR DIGITAL OVERLOAD

- **Set time limits on your use.** For example, set an alarm that reminds you to put your device down after 30 minutes.
- **Use only one device at a time.** If you're on your computer, for instance, turn your phone off and set it aside.
- **Turn off unnecessary notifications.** This includes notifications from social media.

- **Plan your social media and news activities.** Instead of looking at your favorite social media and news sites throughout the day, check them once or twice a day at scheduled times.
- **Prioritize off-screen activities.** Take a walk, play a game with your family, or try cooking a new recipe.
- **Create tech-free times.** Plan to stop using your device at a certain time each night. Using your device’s “do not disturb” function will keep your device-free time from getting interrupted.
- **Create tech-free zones.** For example, make the dining table a tech-free zone in your home.

A little bit of information and healthy screen-use habits will give you the benefits of technology while helping maintain your physical and mental well-being.

Addiction

The following has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)

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 internet addiction, you can ask your doctor for a referral to an experienced therapist who will be able to give you more advice.

Scams, manipulation or hacking

The following has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)

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.

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

Online misunderstandings


The following has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)

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.

Online dating and romance scams

The following has been taken from [Online Dating and Romance Scams | The Office of Attorney General Keith Ellison \(state.mn.us\)](#)

A recent study indicates that 15 percent of American adults use online dating websites or mobile applications. As the number of people looking to meet new people online grows, so does the opportunity for fraud.

Some scam artists use bogus profiles to con the people they meet out of hundreds or thousands of dollars. Criminals who perpetrate online dating and romance scams use emotional appeals to quickly gain their victims' trust and then, just as quickly, exploit it. This leaves many victims not only embarrassed but also in financial distress. It is important for online users to be on the look-out for online dating and romance scams. It can happen like this:

“Maria” signed up for an online dating service and was contacted by “Andrew,” who claimed to be an American overseas on business in Australia. Maria and Andrew seemed to hit it off and began planning a road trip for that summer when Andrew would come back to the U.S. Andrew sent Maria a check for \$5,000 to cover the cost of their trip, but then suddenly asked her to send \$4,500 back to him because he needed money for rent after being laid off from his job. Maria deposited the check and sent the money, but was soon contacted by her bank, which told her the check was bad and she had to repay the \$4,500. On top of losing her money, the fake “Andrew” disappeared, and Maria never heard from him again.

THE PHONY PROFILE ROMANCE

Romance scammers often create a phony profile. The scammer may use photos from magazines and portray himself or herself as talented and successful. Fake profiles may have discrepancies or inconsistencies, like disproportionate height and weight, or be suspiciously vague. Romance scammers often claim to be a U.S. citizen working or serving abroad, or give a similar excuse to explain their inability to meet in person.

GAINING VICTIMS' TRUST

Online dating and romance scams often begin like any other online relationship: interested individuals exchange basic information, like their line of work, their city, and their hobbies and interests. Scammers may then ask their victims to leave the dating site and use personal email or

instant messaging (IM). Con artists may express their “love” quickly and effusively, find similarities with the victim, and claim the online match was destiny.

This is all a build-up for the scam artist’s real goal: conning a victim out of money. Once the victim becomes attached, the scammer looks for ways to dupe the person into sending money, which can happen in two basic ways. In the first scenario, the scammer may indirectly ask for money. For instance, some romance scammers express concern about their financial situation or ability to visit the victim in the hopes that a person will offer to send funds. In the second instance, the scammer asks for money directly. A scammer may beg for hundreds or thousands of dollars, claiming a family member became suddenly ill, he or she was robbed, or the person is having difficulty obtaining travel documents after spending all his or her money on a plane ticket to visit you. A victim may even get a call from an accomplice who claims to be a lawyer or doctor to lend credibility to the tale.

Be wary of sending money to someone you have never met in person, especially via a wire transfer service, like Western Union or MoneyGram, or a prepaid money card, like Green Dot. Once a person wires money to a foreign country, the money is generally unrecoverable.

PROTECTING YOURSELF

Online dating and romance scams are sophisticated operations that are typically conducted by criminal gangs. Con artists share information about victims and may target victims more than once. Some scammers induce victims to share personal information or images and then threaten to post or distribute them to the friends, family members, and employers if the victim refuses to pay.

The Attorney General’s Office encourages people to exercise an appropriate level of caution when looking for a relationship online and to be careful about sharing personal information and photos with people they have never met.

THE FOLLOWING ARE SOME TIPS ON HOW TO PROTECT YOURSELF FROM BEING SCAMMED AND WHAT TO DO IF YOU BECOME A VICTIM:

- **Be careful about sharing sensitive personal or financial information** with someone you have not met in person.
- **Stay on the dating site**—romance scammers ask their victims to use personal email or instant messaging to keep their schemes under law enforcement’s radar.
- When using an online dating site, **use a separate username and different email account** to protect your privacy.
- **Be wary of “coincidental” similarities** as well as inconsistencies in an individual’s story. If things don’t add up, press for details, or ask a friend or family member for their perspective. Romance scammers know that emotions can skew judgment and count on affection and attention to thwart their victims’ judgment.
- **Wiring money is the same as sending cash**—once the money is sent, it is generally lost for good.
- **If an online prospect claims to be a United States citizen living or working in another country and asks you for help or money**, refer the prospect to the local U.S. Embassy or Consulate. If you want to send money, consider a U.S. Department of State Office of

Overseas Citizens Services (OCS) Trust. An OCS Trust works like a wire transfer, but the embassy or consulate holds the money until the recipient picks it up—and provides proof of U.S. citizenship.

- As a final effort, **romance scammers may claim to still be “in love” when they are found out by their victims.** Don’t fall for it. Report scammers to the dating website so others won’t be drawn in.

TAKING ACTION

If you are a victim of an online dating or romance scam, take the following steps:

- Cease all contact and block phone numbers, IM accounts, and email addresses.
- Keep copies of all communications.
- Report the matter to the dating website.
- Report the matter to your local police.
- Report the matter to the FBI’s Internet Crime Complaint Center at www.ic3.gov.
- Report the matter to the Federal Trade Commission as follows:

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue NW
Washington, DC 20580
(877) 382-4357
TTY: (866) 653-4261
www.consumer.ftc.go

Catfishing & Sextortion

The following has been taken from [Catfishing \(cybersmile.org\)](http://catfishing.cybersmile.org), [The 5 Types of Catfishers You May Encounter Online - Social Catfish](#), [Catfishing \(cybersmile.org\)](http://catfishing.cybersmile.org), [Prepaid Debit Card Scams | The Office of Attorney General Keith Ellison \(state.mn.us\)](#), [Owner of Social Catfish Breaks Down Online Dating Scams \(aarp.org\)](#), [Catfishing \(cybersmile.org\)](http://catfishing.cybersmile.org), [What Is Catfishing? 7 Signs of the Romance Scam \(rd.com\)](#), [Five Coronavirus Scams Impacting Disabled People \(disabilitydetails.com\)](#), [Internet and phone scam alert for disabled people. Be aware \(brrlaw.com\)](#), [Catfish-buster warns of trending scam infiltrating Facebook Marketplace \(yahoo.com\)](#), [Debt Collection Scams | Office of the Attorney General \(texasattorneygeneral.gov\)](#), [7 crimes that have become possible with the advent of the Internet \(virilejournal.com\)](#), [2022 Snapchat Scams: Don't Fall For These 7 Devious Tricks | Aura](#) and [Google Voice Scam Tricks You When Selling Online - ITRC \(idtheftcenter.org\)](#)

Catfishing is when someone uses images and information (often taken from other people’s social media accounts) to create a new identity online – sometimes using an individual’s entire identity as their own. Newly created social media accounts can then be used to damage the reputation of the true owner of the identity, or alternatively any fictional identities that are created using other people’s images and information can be used to form dishonest relationships online. Although catfishing used to be seen more among adults using online dating platforms, it has now become a more widespread problem among adults and teenagers. Some people who catfish go to extreme lengths to create fake identities – having multiple social media accounts with the purpose of building up and validating their catfishing profiles.

One of the ways catfish victimize individuals is by **sextorization**, which is the threat to expose intimate photos, videos or other communication of/ from the victim as coercion to something, such as money. Often, these are bluffs. However, they can put a very heavy emotional toll on the individual experiencing them.

5 TYPES OF CATFISH YOU MAY ENCOUNTER ONLINE

- **Romantic Catfishing:** This is one of the most common types of catfishing. It involves creating a fake profile on dating sites or social media platforms to lure someone into a romantic relationship. The catfisher might use fake photos, personal details, and interests to create an appealing persona.
- **Financial Catfishing:** This type of catfishing is aimed at tricking someone into giving money or other valuables to the catfisher. This can include setting up fake crowdfunding campaigns, pretending to be a charity or a business, or posing as a wealthy individual to gain trust.
- **Identity Theft Catfishing:** This type of catfishing involves stealing someone else's identity to create a fake profile. The catfisher might use the victim's personal information, such as their name, photos, and social media accounts, to create a convincing fake identity.
- **Cyberbullying Catfishing:** In this type of catfishing, the catfisher creates a fake profile to harass or bully someone online. They might use insulting or threatening language, spread rumors, or post embarrassing photos or videos.
- **Revenge Catfishing:** This is when someone creates a fake profile to seek revenge on someone they know or used to be in a relationship with. They might use the fake profile to spread lies or rumors, or to publicly embarrass the victim.

SIGNS THAT YOU MIGHT BE BEING CATFISHED

It can be difficult to spot a catfish. Although the signs you might be getting catfished can be different for each situation, some of the most common signs that you could have fallen victim to catfishing include:

- **They don't have many friends or images on their social media accounts** – When someone is catfishing, they will have to take the photos they choose to use from another source. Most commonly, they will take images from someone else's social media account. Because the images are taken from an authentic source, catfishers have no control over when or what is posted so they will only have access to a few images at a time – when the 'real' person shares images themselves. They might also have very few friends and show little or no interaction with them online.
- **They never want to video call** – Someone who is catfishing, will not want to video call if they are using another person's identity. In order to avoid video chatting, catfishers make up excuses. They might say their webcam is broken or they're always too busy.
- **They don't want to meet up** – For obvious reasons, catfishers will never want to meet up. To avoid this, some catfishers will agree to meet up with you (to seem more authentic) only to back out at the last moment.
- **If they don't use Snapchat** – It sounds strange but Snapchat has now become so popular that if somebody is active on various social media platforms but doesn't use Snapchat, this could be suspicious. Snapchat is based around sharing 'live' selfies – making it impossible to use images

taken from other people’s accounts. If you are being catfished, they might say they don’t use snapchat or add you on it and then refuse to send you a photo of themselves.

- **Nonstop chatting** – Catfishers want to quickly figure out if they’re building trust or if the victim is on to them, so they love bomb all day and night. “More often than not, catfishers will contact their victims at odd hours of the day,” says Rori Sassoon, a relationship expert, author of *The Art of the Date* and co-owner of matchmaking agency Platinum Poire. “They may use the excuse of being in a different time zone.”
- **Inappropriate requests** – A potential love interest won’t generally request explicit photos at first, but a catfisher might constantly make this request because they’re looking for a way to blackmail you. “The explicit content and other sensitive information make it easy for them to steal from you,” Santini.
- **Intentionally vague communication** – Some people don’t engage with social media, and on its own, that’s not alarming. “But something shady is going on if they refuse to tell you their last name or have a nonexistent social media presence,” Sassoon says. “And that’s the last thing you want to be involved in.”

Catfishers will never reveal details that you can prove—that’s one of the prime ways to identify a scammer. They keep their responses generic and are intentionally vague so you can’t detect outright lies. They’ll tell you they live “outside of Boston” but won’t give you an exact town, or they might tell you the city where they (supposedly) went to college but not the name of the school.

“You can’t track them to an address or a desk at their office or their job,” Trombetti says. “Maybe their name is a very common one, so it’s hard to Google them and find out if they’re really who they say they are.”

- **Awkward or unrealistic photos** – If your new beau is sharing photos of his dog but something about them seems off, trust your gut. A photo stolen off the web might be blurry or cropped oddly. “Scammers are after low-hanging fruit,” Eaton says. “So they usually don’t take the time to edit and Photoshop the images expertly. They’re trying to do the least amount of work possible.”

Unrealistic photos are another telltale sign. “Most of the people you meet on social media sites aren’t going to look like supermodels,” she says. “Their bodies won’t be shredded, ripped and perfectly tanned, with all their pictures looking like they were taken on location by a professional film crew. I mean, it’s possible that a Victoria’s Secret supermodel is lonely and desperate to meet you, but it’s probably not the most high-probability outcome.”

It’s worth noting that some scammers also use software driven by artificial intelligence to create personalized images of people who don’t exist so you won’t be able to find their photos on the web and see that they belong to someone else. “Most scammers aren’t this sophisticated,” Eaton says. “But it’s coming.”

- **The person is too good to be true** – When it comes to online dating, anyone who seems too good to be true generally is. Scammers have mastered the art of scouring accounts for details, which means your so-called girlfriend will likely share many of your interests. “They pretend to

want the same things out of a relationship that you do because they are trying to gain your trust so that they can rob you of your money,” Trombetti says.

- **Text- only communication** – Texting has become increasingly common—some people use more texting shorthand and emojis than actual words. But if you’ve been texting with a new “online friend” for a few weeks, you’ll get to the point where it makes sense to hear each other’s voices and have an actual conversation. If they won’t, it’s a warning sign.

Of course, *you can keep an eye out for warning signs in text conversations as well.* “There are chatbots that initiate and mimic text conversations, but you should be able to tell that their responses aren’t on the level,” Eaton says. “Usually, they’re clumsy at redirecting the conversation, understanding references and answering personal questions. They’re great at asking questions—but not nearly as proficient at answering them.”

- **The person redirects you elsewhere** – Let’s say you receive a message from a would-be romantic partner, who then asks you to visit an *OnlyFans* account (*OnlyFans* is a social media platform where content creators can share various forms of content. Often times, this site is associated with sharing pornography). Could it be legit? Maybe. There are two possible reasons someone might message you but direct you to an *OnlyFans* account: They might be on *OnlyFans* and want you as a member of their fan base. Or they stole photos from someone and are catfishing you.

“It’s possible that the *OnlyFans* star is romantically interested in you, and it’s also possible that your ‘personal’ message was mass-blasted to thousands of people,” Eaton says. “And it’s further possible that their *OnlyFans* URL is a phishing attempt to take you to a bogus website and steal your financial data.”

Bottom line: Don’t click on links in messages.

- **The person requests money from you** – Scammers like to have money transferred to them in ways that allow the scammer to be long gone before the scam is detected. For the same reason that scammers often ask money to be wired to them in another country (that is, they’ll be long gone with the wire transfer before the consumer spots the scam), scammers may ask that money be given to them using a prepaid debit card. They may wait until the victim has fallen romantically for them to make their move. and might even avoid asking for money outright, instead asking for a “loan” or a “temporary advance” with a promise to return the money (which does not happen).
- **The person quickly begins romancing you** – Scammers groom victims by showering them with compliments, sending love poems, professing their undying support and even mailing small gifts with love notes attached. Some experts refer to this as love bombing. The goal is to get the victim so infatuated with the scammer – or more accurately, the character he or she portrays – that the victim will be more likely to say yes when asked for money.

Although most people feel confident that they would know if they were communicating with a completely fabricated identity, it is also very easy to assume after seeing a few images and some conversation that you are communicating with exactly who you are looking at in the images! It is

important to remember that although many of the signs that you are being catfished listed above can be indicative of something sinister – they can also be completely innocent too.

STRATEGIES FOR CATFISHING

Avoiding getting catfished can be very difficult, because of the sheer volume of people we interact with online each day. Therefore, it can be difficult to check each identity for authenticity. However, there are tips to prevent or reduce your chances of being catfished. Some of the ways you can prevent being catfished are:

- **Be cautious** – When talking to anybody that you don't know online, always remain slightly cautious, especially if you have only just started speaking with them or have no solid evidence that they are who they say they are.
- **Never give out money** – Some catfishers will target people in order to scam money from them. You should never give money to anybody who asks for it online.
- **Take your time** – Always be careful when sending images or sexually explicit messages to another person online. Once you press send, it can't be taken back!
- **Talk to someone** – If you have concerns about someone you are speaking to online, confide in someone you trust. Tell them about your concerns as they may be able to help you identify any "red flags" you may have not noticed yourself. New perspectives often bring new solutions!
- **Don't be afraid to ask questions** – As uncomfortable as it might be, don't be afraid to ask as many questions as you need to in order to feel comfortable talking to someone. If they are a catfish, they might not be able to answer all the questions accurately and then you'll be more likely to know that something isn't right.
- **Adjust your privacy settings** – Catfishers will commonly look for potential victims to target, and by having your privacy settings adjusted on your social media accounts to 'private', you are less likely to fall victim to catfishing because nobody can see the information on your profile.
- **Don't click on any links the person sends**—it's most likely a phishing attempt. If you did click a link, beef up your online security with strong passwords to make sure the fraudster can't access your accounts.
- **Stop communicating with the person immediately.** Trust your gut.
- **Block this person and don't explain yourself.** Just go.
- **If you need actual proof, use Social Catfish to verify the person's identity.** Keep in mind that even if your search comes up blank, you might still be getting catfished.
- **Report the person's profile to the dating app or social media site** where you met.
- **If your financial information is compromised, notify your bank and credit card companies immediately.**
- **Report the scam** to local law enforcement and, if you're down six figures or more, report it to the FBI.

POPULAR CATFISHING SCHEMES

- *(Often seen on Facebook)* **The scammer will respond to a post for people selling items online.** The scammer pretends to be a buyer, responds to your post shortly after going live, and state they are interested and want to buy. They then ask if they can call you to ask for additional details and explain that you will have to respond to a **Google Voice verification code** that they

send to verify that “you are a real person.” Once they receive this code, they can create a fake Google Voice account in your name which they use to scam others.

- **The scammer will call or email a Medicare and Medicaid beneficiary, claiming to be Medicare or Medicaid representatives asking for their personal information.** Medicare or Medicaid would never call for email you from an individual account asking you for your personal information. In fact a Medicare or Medicaid representative would never do any of the following:
 - call you to ask you to verify your Medicare or Medicaid number,
 - call you to try to sell you anything,
 - promise you something in exchange for sharing your Medicare or Medicaid number
 - visit you at your home
 - call you to enroll you in a Medicare or Medicaid program unless you called them first
 If you receive a call or an email from someone claiming to be a Medicare or Medicaid or representative, hang up or delete the email.
- *(Often completed on the phone)* **The scammer calls the victim and claims they owe the IRS money and they need to pay immediately.** The caller will threaten anything from a lawsuit to incarceration if the victim does not make a payment over the phone. Other scammers will take a different approach and say the victim is entitled to a huge refund if they simply make a small payment now.
- This scam involves targeting people collecting Social Security benefits. **The scammer calls or emails the victim and claims to work for the Social Security Administration (SSA) and told victims that they had been underpaid, and they would need to provide their bank account information in order to receive their money.** Similarly, there have been other reports regarding a [scam](#) which told victims they could receive a \$2,000 per month grant for a payment of \$750. Some scams don’t demand a payment up front. Some scammers are clever enough to convince their victim to give up their personal information, and then the criminal is able to reroute the Social Security benefits to himself.
- *(Often seen on Facebook)* The scammer will respond to a post for people selling items online. They pretend to be a buyer, respond to your post and agree immediately without negotiation, no questions asked about the price or the item. **They’ll then offer to pay you through a money transfer app, but claim it didn’t go through because you need to update your account.** The scammer will send you a link asking you to pay a fee, claiming that it’s required to allow the money to go through or using similar wording, which will be followed by a fake email from the company asking you to confirm.
- **The scammer will create posts and advertisements online to sell an item, rent a room or look for a lost pet.** The victim reaches out because they are interested and the scammer requests a **Google Voice verification code.** Once they receive this code, they can create a fake Google Voice account in your name which they use to scam others.
- *(Often seen on Snapchat)* **The scammers pretends to be one of your friends who needs help recovering their account.** They’ll ask for your account login information, so they can look through your *Friends List* to “remember” their username. Give them access to your username and password, and they’ll take over your account.

- *(Often seen on Snapchat)* **In this scam, your friend’s hacked account will message you about an “advertising gig” or influencer sponsorship on a social media account.** They say they already made hundreds or thousands of dollars, and you can too. All you have to do is send them a deposit (cash, Bitcoin, or gift cards) to cover the cost of signing up. Then they’ll disappear as soon as they receive it.
Other times, scammers will ask for your login information to “set up” the sponsorship or “promote” the advertising opportunity for you. Then they’ll take over your account. They’ll also start posing as you to repeat this scam to everyone on your friends list.
- **The scammers create a shocking Facebook post that will gets lots of shares (like missing or abused animals) and then turn off the comments.** After it gets so many shares, they edit the post to something that drives traffic to a bogus website that steals your info.
- **The scammer sends a text message posing as your financial institution. The text claims to be “urgent” and falsely says your debit card account is locked. They provide a phone number to call to “unlock the card.”** Cardholders who call the number provided reach an automated menu with a computerized voice. They are then asked to provide their personal card information—full card number, expiration date, security code on the back of the card, and their PIN. The fraudster then tells the customer they will receive a code via text message on their phone, and they are to give that code to the scammer. BUpon receiving this code, the scammer now has a digital version of the customer’s debit card on their own phone.
- **The scammer contacts you — often by phone, but also by text message, fax, mail or email — and claims that you owe a debt.** The debt may be completely fake, canceled, discharged, forgiven or beyond the period for collection. The scammer then uses all sorts of techniques to get you to pay such as intimidation, lies, threats, harassment.
Before you pay any debt to any collector, confirm that the debt is real and valid.
- **The scammer sends a text message stating that a package (from UPS, USPS, Fed Ex) could not be delivered because the wrong zip code was on the order.** They then state it can be redelivered if you pay “30 cents” (or other amount) postage or it would be returned and need the credit card numbers to get it delivered.
If you feel this could be a real possibility, go to the nearest UPS, USPS or FedEx and show them the text to confirm if payment is needed. Never give your card numbers out over a text message or email.
- **The scammer sends an email to you explaining that they have been watching you and have recorded your actions (usually sex related) or they might say they have an intimate photo of you (or one that you may have provided to them). They request that you provide them their request, and if you don’t complete it; threaten to publicly share your video, photo or communication on an online forum.** Often times, they provide a short deadline for the turnaround.
If you get such a letter, it is best to ignore it since the odds of following through on this threat is rare. Additionally, it is best to change passwords from social networks, mail and messengers and update spam filters that block unwanted mail.

- **The scammers strike up a relationship with you to build up trust, sometimes talking or chatting several times a day.** Through little conversations, they get bits of information from you such as your full name, address, phone number, etc. As a result, it can be difficult to recognize this as a red flag based on the type of information they are trying to get out of you. Often, they push for a relationship which can include expressing feelings of love, wanting to move in with you, marry you, or ask to have online sexual experiences (which could also include requesting explicit photos of you). They will ask for money and make up a story that will strike emotion in you (e.g., they need help paying medical bills for them or a family member, they want to buy a ticket to come and visit you, they are in legal trouble and need the money so they don't get into trouble, etc.). They may even offer to help you get started in cryptocurrency investing. Since they want to get the money quickly and in a way that is difficult for you to get back, they will tend to request that you wire the money through a company like Western Union or MoneyGram, put money on gift cards and send them PIN codes, send money through a money transfer app, or transfer cryptocurrency. If you give them money, they create another scenario where they need more money. If you happen to decline their request, they will quickly escalate and might threaten to broadcast private information or explicit photos of you in online forums, to your friends and families, workplace, and other places unless you pay them money.
- These are scenarios that can cause financial and emotional harm to its victims due to the false relationship they appear to create. Often, the victims refuse to believe they were ever scammed and that they really did have a relationship with the person. Unfortunately, scammers do these things to get involved with your emotions so you trust them and then pressure you into acting immediately by paying money.**

Bottom line, never send money or gifts to anyone that you have not met in person.

If you fall victim to a Google Voice scam, you should reclaim your number. [Click here to learn more.](#)

For more information on the Google Voice verification scam, or if you believe you are a victim, contact the ITRC at no cost by phone (888.400.5530) or live-chat on the company website idtheftcenter.org.

Check to see if a recent data breach gave hackers access to your personal information on the Dark Web with Aura's [Leaked Password Scanner](#)

Phishing emails

The following information has been taken from [How to Recognize and Avoid Phishing Scams | Consumer Advice \(ftc.gov\)](#), [Safety online: A guide for people with autism spectrum disorder \(openmindschool.org\)](#), [Safety online: A guide for people with autism spectrum disorder \(openmindschool.org\)](#), [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)

Scammers use email or text messages to trick you into giving them your personal and financial information. At first glance, this email looks real, but it's not. Scammers who send emails like this one are hoping you won't notice it's a fake.

While real companies might communicate with you by email, legitimate companies won't email or text with a link to update your payment information. Phishing emails can often have real consequences for

people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

But there are several ways to protect yourself.

HOW TO RECOGNIZE A PHISHING EMAIL

- **It looks like it's from a company you know and trust.** It might even use the company's logo and branding.
- The email says your **account is on hold because of a billing issue.**
- **It has a generic greeting like "Hello."** If you have an account with the business, it probably wouldn't use a generic greeting like this.
- The email **invites you to click on a link** to update your payment details.

[The FBI recommends](#) mitigating these risks by using a firewall, keeping your antivirus software up-to-date and shutting down your computer when you're not using it. It's always a good idea to double-check the email address that sent you a message before clicking any links or opening attachments.

Cyberbullying

The following information has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)



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.

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.

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 steps 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.

Pornography

The following information was taken from [Autism and Child Pornography | Law Office of James R. Snell, Jr., LLC \(snelllaw.com\)](#), [Promoting Internet Safety Among Users with Autism Spectrum Disorders \(worksupport.com\)](#)

The world of pornography is an easy way for people to access and explore their questions and interests about sex. Unfortunately, these sites can easily lead to the dark web, even when the user is not intending to explore it. This danger increases significantly when the person seeking pornography lacks a certain level of knowledge, abilities, and/or skills. Individuals with **autism** are more likely to unintentionally fall into this trap if they are social isolated, have an inability to understand or appreciate socially expected boundaries, lack the understanding of the “wrongness” of their behavior and or lack sexual education, and are not taught about the legalities of these types of websites. Education and knowledge are a necessity for everyone who has an interest in these websites, to allow them to explore their interests while keeping them safe. As a supporter, it is important to be proactive and provide instruction to understand pornography and the realities that are not often considered.



People with **ASD** absolutely must have explicit and accessible sexuality education. This includes teaching people about pornography.



SOME TOPICS TO COVER INCLUDE:

- **Legal vs. illegal images.** Images of children will get you arrested.
- **Exploitation.** Children have been hurt in the making of pornography.
- **Social perception.** What do other people think about the use of pornography? Is that information to share with others? If yes, when and with whom?
- **Skewing body images.** Real people don't look like that. You do not look like that. Your partner will not look like that.
- **Pornography is fake.** It is not an example of real relationships or real life.
- **Relationships develop over time.** Physical and emotional intimacy increase gradually.

Legal traps for internet pornography users: 5 ways you can get in trouble

The following information was taken from [Legal traps for internet porn users](#)

There are many ways in which the mere viewing of adult internet pornography can get you in trouble. Many pornography users and pornography addicts are unaware of these legal traps or choose not to think about them.

But even if the pornography has entirely adult content and even if there are no real children depicted anywhere in it, there are ways pornography addicts and pornography users can get in trouble.

YOU MAY BE LOOKING AT CHILD PORNOGRAPHY AND NOT REALIZE IT

Under current US law, the definition of child pornography has been expanded to include digital images and images where there is no actual child involved. It has also been expanded to include photographs, videos, digital or computer generated images indistinguishable from an actual minor, and images

created, adapted, or modified, but appear to depict an identifiable, actual minor, undeveloped film, undeveloped videotape, and electronically stored data.

AFFIRMATIVE DUTY TO REPORT SOMEONES USE OF PORNOGRAPHY AT WORK

According to the 2010 Nielson Company survey 29% or 21 million Americans access pornography at work. There are a number of dangers inherent in watching adult pornography sites at work:

Downloading adult content can lead to malicious software on your computer that loads pornography onto your home page every time you log on. At the very least this means that you will be exposed, at least to your IT person.

Harassment: if another employee has complained about your pornography use the employer has a legal obligation to change the situation. If you work in a non-government job, there is no federal law that prohibits employers from searching an employees computer.

If child pornography is found on your workplace computer your employer has a legal responsibility to report you to the National Center for Missing and Exploited Children.

Some states have passed legislation that makes viewing pornography on a school districts computer reason to revoke a teachers license. Teachers generally are particularly likely to lose their jobs over pornography viewing.

THINKING ONLY PORNOGRAPHY YOU DOWNLOADED COUNTS

Possessing child pornography is a violation of federal law, but some people still make the mistake of thinking that they are not in possession of child pornography if they viewed it but did not knowingly download it (i.e. if it was cached by their computer automatically.)

Lack of knowledge has worked in overturning a child pornography possession conviction but the federal law actually criminalizes any act of accessing or attempting to view child pornography. (The law allows for a defense of accidental viewing if you view less than 3 images and delete them immediately.)

PHOTOGRAPHY CAN BE PORNOGRAPHY PRODUCTION

Nude photos are not necessarily deemed erotic content. But you are on shaky ground with photographing your teenage girlfriend in erotic poses. You need also to be aware of federal criteria in the law cited above that classifies pornography as child pornography when it depicts content in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

The law says that Congress has made a clear determination that pseudo-child pornography places children at risk by encouraging certain behaviors and being susceptible to invidious uses by pedophiles to harm children.

PROFESSIONAL REPORTING LAWS

All states have laws requiring the reporting (to child protection/law enforcement) of child abuse and neglect by professionals. 48 states list who these mandatory reporters are (such as medical

professionals, therapists and teachers.) New Jersey and Wyoming have mandatory reporting laws but do not list specific groups of professionals.

You can look up the specifics of the law and of the state requirements for any state, but many state laws do not require professionals like therapists to report pornography viewing that is in the past and where there is no suspicion that a child is currently endangered.

States also vary as to the mandatory reporting of crimes that people hear about in their professional capacity. This means that in some instances, the pornography related crime may be the possession of pornography or child pornography or related offenses that are on the books in that jurisdiction.

As I have reported previously, there are still laws on the books from the Bush era that allow for the prosecution distributors of hardcore adult pornography.

Prosecution of such cases is a rarity but pornography addicts and pornography users need to figure out the reporting requirements for their state and make a judgment as to where their therapist stands on weighing confidentiality vs. required reporting.

TIPS & STRATEGIES SPECIFICALLY FOR CHILDREN, TWEENS & TEENS

Although these are designed for children and teens, these resources can be used with adults, depending on their level of knowledge and understanding. Additionally, a number of these resources can be generalized to other ages and populations as well.

General tips & strategies specifically for families with children & teens

The following information has been taken from [Promoting Internet Safety Among Users with Autism Spectrum Disorders \(worksupport.com\)](#), [C3P Parenting in the Digital World en.pdf \(protectchildren.ca\)](#)



Many individuals with **ASD** a lot of time on the Internet. However, these individuals may not always understand the dangers that are present online or the issues they can get into online. As family members, we must educate ourselves on these issues and, in turn, educate our children.

IMPORTANT INFORMATION TO KNOW:

- Know what **apps** your family member accesses.
- Know how to **operate the devices** that are present in your home.
- Set up an **Internet safe home** (filters, virus protection, parental controls, child friendly browsers)
- Set up and post **family rules** for Internet usage.
- Check and double-check what **websites and apps** your family member is visiting.
- Teach your family member what can get them **arrested**.
- Know your family member's **accounts and passwords**.

Common internet safety rules for children and teens

The following information has been taken from [Internet Safety for Kids | Parents' Guide to Keeping Kids Safe Online \(consumernotice.org\)](#)

Parents are the best suited to monitor kids' online activity. They are also the most trusted adults most kids will turn to if they experience online dangers. Understanding what your children or teens do online is vital to protecting them from digital threats.

STRATEGIES TO TEACH YOUR CHILDREN FOR SAFE INTERNET USE:

- **Never give out personal information**, including your name, address, phone number, social security number or home address
- **Do not post your photo** on public sites of any kind
- **Do not chat** with strangers
- **Don't open an email** from someone you don't know
- **Don't respond** to hurtful, insulting or bullying messages
- **Report inappropriate messages** to a trusted adult

- **Never agree to get together** with someone you've only met online
- **Set limits** for being online

PLAY IT SAFE acronym to teach teens with ASD about internet safety

The following information has been taken from [Internet Safety for Adolescents with Autism.pdf \(unc.edu\)](#)



To teach teens with **ASD** about internet safety, an acronym called PLAY IT SAFE can be helpful (adapted from Cerebra.org).

P - Personal information-don't share it, never give out your full name, where you live, or where you go to school

L - Let a trusted adult know-tell someone if anyone asks for your personal information

A - Attachments-beware before opening any attachments

Y - Your feelings are important-if something happens that makes you uncomfortable, tell an adult right away

I - Information-remember that not everything you see online is true. If you are unsure ask a trusted adult

T - Take breaks from the computer-it is important to take breaks so that you don't strain your eyes and so you also have a chance to talk to other people and do other things. Set a timer to ensure you are not on the internet too long

S - Spending money online-don't buy things without permission. Money should only be spent by a trusted adult

A - Act politely-don't say anything online that you would not say to someone in person

F - Friends online should stay online-if someone asks to meet you, tell them no and always let an adult know

E - Enjoy yourself-Play safe and have fun!!!

Discussions parents should have with their tweens and teens

Make it a habit to talk with your tween/teen about online activities.

DISCUSS THINGS LIKE:

- The **privacy controls** they have set up on the various apps they use.
- Who they are "**friends**" with on social media and how they know them.
- Who they **chat** with and/or video chat with online.

- What **information they should and should not be revealing** in their messages, posts and photos/videos.
- The fact the Internet is a public space and it's **easy to lose control over** what happens to texts, photos and videos sent through apps and social media.
- If they've received any **unusual requests online** or if they've ever felt uncomfortable with an online interaction, and how they handled it.
- If any of their friends had a **difficult experience online**, and their feelings around what happened.
- Being a leader and **not forwarding pictures** of others they may receive.

TALK TO YOUR TWEEN/TEEN ABOUT PAYING ATTENTION TO UNHEALTHY BEHAVIORS SUCH AS SOMEONE WHO:

- Persistently asks for **sexual content** (i.e., intimate pictures/videos).
- Tries to use **pity/guilt** to have them comply with a request.
- Tries to use **content or information shared in confidence** to try to embarrass or hurt them.
- **Doesn't seem to take "no" for an answer** (persistence).
- Seems to be **sharing overly personal information** too quickly.
- **Offers money/gifts** to try and get them to do something that makes them feel uncomfortable.
- Remind them **healthy relationships** involve mutual caring and respect. Without a clear understanding of what makes a healthy relationship, teens are more likely to tolerate relationships that put them at risk.

CONSIDER REVIEWING THE FOLLOWING WITH YOUR TWEEN/TEEN:

Explain that adults should not seek out friendship with teens or give them any type of sexual attention. This inappropriate behavior at a minimum shows poor judgement and therefore makes it unsafe to interact with that adult.

Talk with your child about the importance of seeking help from you if they are uncomfortable with any exchange with an adult. Even if they are embarrassed, reinforce you are there to help.

DISCUSS DIRECT AND INDIRECT WAYS OF GETTING OUT OF UNCOMFORTABLE SITUATIONS:

- **Tell it like it is:** "No way." "I don't want my pictures all over the Internet." "Forget it."
- **Make a joke:** Humor may help change the topic and ease your tween/teen out of the situation.
- **Make up an excuse:** "Sorry, I have to go out." "My mom checks my phone randomly so I can't."
- **Ignore:** Explain there is no need or urgency to respond to any messages, especially messages that make your tween/teen feel uncomfortable.
- **Stand your ground:** Teach your tween/teen to repeat their answer if someone is not listening. Explain that persistence is controlling behavior. Encourage them to be firm in their response and if that doesn't work just stop responding.
- **Block all contact:** The option always exists to block or delete the individual. Also, it may be important for your child to save the messages in case at some point you need to show the communication to the school and/or law enforcement.

- **Report it:** Most social sites and apps have a reporting mechanism that can be used to report inappropriate behavior by another user. Talk with your tween/teen about these features and encourage them to use it when needed.

HELP YOUR TEEN IDENTIFY EXAMPLES OF WHEN A SITUATION HAS GONE TOO FAR, SUCH AS:

- When communication with someone starts feeling uncomfortable and/or feeling like a mistake has been made.
- When an individual starts makes lewd and offensive comments.
- Situations that start as harmless and fun but become uncomfortable, excessive, stressful or scary.
- When intimate pictures or videos are circulating without consent from the person in the picture/video.
- When communication with an adult has become sexualized or inappropriate. While it isn't unusual for a teen to develop a "crush" on someone older, it is inappropriate for an adult to have a "crush" or sexual interest in a teen. It is the adult's job to establish and reinforce appropriate boundaries.
- When the communication involves threats or blackmail.

Exposure to inappropriate content

The following information has been taken from [A Helpful Online Safety Guide for People With Autism Spectrum Disorder – TheTouchPoint Solution™](#)

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

- **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 the '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](#).

- **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.

- **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.

- **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.

- **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 emails 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.

Online luring

The following information has been taken from [Online Harms: Online Luring – Cybertip.ca](#)

Online luring is when a person (typically an adult but not always) communicates with youth through technology, like texting, direct messaging, or chatting in an app/game/website, to make it easier to commit a specific sexual offence against them.

An example of a communication that may be reported as luring is if the person asks, hints at, or tries to convince the child/youth to create or send naked or semi-naked sexual pictures or videos.

Adults looking to exploit youth use a number of tactics to groom teens online, such as sending sexually explicit material, misrepresenting who they are (e.g., saying they're also a teen), or attempting to establish a romantic relationship. This coercion is used in hopes the youth will either meet the offender in person or send sexually explicit material, which may be used to blackmail or extort the teen.

STRATEGIES AND LESSONS

- Explain what online luring is and how it happens.
- Ask your youth why they think this is a criminal code offence in Canada. Listen to their perspective and discuss the importance of laws to keep youth safe online.
- Teach them about red flag behaviors that signal a situation is unsafe.
- Discuss how to get out of conversations and/or online relationships when they feel uncomfortable. Discuss direct messaging (e.g., "I don't want to" followed by deleting or blocking

the person) and indirect messaging, such as making up excuses (e.g., “My mom checks my computer randomly and would ground me”).

- Emphasize the importance of getting help – coming to you or another safe adult or reaching out to needhelpnow.ca for help. Explain that if this has ever happened or does happen to them or someone they know, you want to know about and want to help them. This is too serious for youth to manage on their own; and the good thing is they’re never alone and it’s never too late to get help.
- Share a real case and, together, identify the red flag behaviors/tactics and discuss what the youth should do. Download. [How to Talk with Teens about Online Luring](#) for more information and a real case example.

Self/ peer exploitation

The following information has been taken from [SPEX FamilyGuide Web single en.pdf \(needhelpnow.ca\)](#)

Self/peer exploitation is defined as youth creating, sending or sharing sexual pictures and/or videos with peers via the Internet and/or electronic devices. Below are strategies parents can use, if they find that their child is involved with this type of situation.

WHAT TO DO IF YOUR CHILD IS A VICTIM OF SELF/ PEER EXPLOITATION:

****Victim of Self:** Youth whose picture/video has been taken and/or distributed, whether by themselves or someone else.

- **Reassure your child**
Reassure your child that s/he is not alone and that together, you will get through this. In the event that you are the first to learn about your child’s involvement in a self/peer exploitation incident, we encourage you to immediately notify and involve your child’s school. They can be an important ally in helping you address the issue
- **Engage in fact-finding**
Ask your child to describe what s/he sent and to whom, how it was sent, when it was sent, and where it was posted/located. This information will assist in guiding your next steps.
Note about viewing content: It is very important that parents do not actively seek out the viewing of the content unless there is a compelling reason to do so. Your child may feel embarrassed knowing that you have viewed a sexual image/video of her/him. For this reason, limiting the number of individuals who see the content is in her/his best interest.
- **Explore the steps your child’s school can take**
Assuming the police are not involved and that the school is willing to work with you, explore the concrete and immediate steps the school can take to communicate with the families of the children involved. As soon as possible, have the content deleted from personal devices and Internet accounts to help contain further distribution of the material. Should police be involved, speak to them about the steps they will be taking. It is important to determine who will be doing what to help remove the content from the Internet in your efforts to minimize any ongoing harm to your child.

Note about supporting your child: You will have to judge what to do to best support your child through this difficult time. It may be challenging for you to avoid focusing on your own feelings of anger, doubt, mistrust and failure. However, it is precisely at this time that your child needs you to be at your best as a parent. Creating a safe environment for your child to talk about what happened will be critical in helping them navigate through whatever challenges they may face.

- **Address the concerning content**

Contact the Website: If the concerning content continues to be publicly available on the Internet (e.g., social networking sites), you can also contact the site directly utilizing the Report Abuse function to request the material be removed (particularly in circumstances that do not involve law enforcement). This feature is available on most of the user-generated content websites. It is important that when you do this, you let the site know that you are the parent, that the person in the picture(s)/video(s) is under 18 years of age and that the content was made available without your child’s consent.

Send a Message: If you do not know whether the concerning content is online or otherwise being shared but are worried that it might happen, or even if you know it is being shared, you may wish to send a message to the parent(s) of the acting-out youth and/or the parent(s) of other involved youth who may have the picture. You may wish to include the following types of statements:

- **Explain the issue:** I have reason to believe [your son/daughter, or insert name of acting-out youth or other involved youth] is in possession of an intimate image of my child. This is a serious and potentially criminal matter. I am reaching out to you with the hope that you will be able to assist in addressing this concern. (You may also wish to include some details such as a description of the picture/video and the circumstances under which it was taken.)
- **State the possession of the image is non-consensual:** State that possession of the image is non-consensual. According to my child, the picture/video was taken in circumstances considered to be private and personal and my child does not consent to [your son/daughter, or insert name of acting-out youth or other involved youth] being in possession of the picture/video. (If the picture/video was initially provided voluntarily, you may wish to adapt this language — for example, by adding the words “any longer.”)
- **Address past/ future distribution:** Address past/future distribution. My child does not consent to [your son/daughter, or insert name of acting-out youth or other involved youth] sharing it with any other person or posting it in any online location. (If distribution has already occurred, you may wish to state that your child did not consent to that distribution, and does not consent to future distribution.)
- **Request deletion:** I request that you speak to [your son/daughter, or insert name of acting-out youth or other involved youth] and ensure that he/she deletes the picture/video and all copies s/he may have of it immediately. In addition, if [your son/daughter, or insert name of acting-out youth or other involved youth] has posted the picture/video in any online or other location, I ask that you ensure that s/he remove the picture/video immediately.
- **Reference possibility of police involvement:** This request is being made now in order to avoid the need to involve police. In Canada, it is a criminal offence (section 162.1(1) of

the Criminal Code) to distribute an intimate image of another person without the consent of that person.

- **Seek confirmation:** Please respond to this message and confirm that the intimate image has been deleted/removed as requested. If I do not receive confirmation from you within [set the number of days — anywhere from 2 to 7 should be enough], I may have no choice but to contact police.
- **Involve your child**
Ensure that your child is apprised of and understands what will happen next. The goal is to ensure that s/he feels empowered and part of the solution.
- **Outline the consequences with your child for the behavior**
While still being supportive, be clear that there are consequences for her/his behavior (e.g., restricted cell phone and Internet use, increased supervision). Discipline should be logical and fit with the behavior and should differ from a punitive approach. Examples may include:
 - **Instructing your child to temporarily suspend use of her/his Facebook® account** to limit harm in viewing other peers' comments regarding the incident.
 - **Temporarily suspending your child's cell phone and/or Internet use** as a consequence for her/his error in judgment and to limit her/his exposure to any online bullying that may ensue.
- **Reassure your child**
Instruct your child not to retaliate against those involved in spreading the content. Reassure her/him that you are working closely with the school to ensure the incident is managed with great care and sensitivity.
- **Reinforce the importance of friends**
Help increase the strength and resiliency of your child by reinforcing the importance of your child's friends in helping her/him manage through this time. They can serve as a protective factor and reduce the likelihood of bullying that may result from your child's decision to share sexual pictures/videos.
- **Create a safety plan with the school**
Work with the school to create a safety plan — you want to ensure that your child is properly supported and feeling secure. This should include your child knowing who to go to for help to address any further problems. The plan should also include what the adults in your child's life are going to do to help keep her/him safe.

Find out what the school knows about the incident, try your best not to react emotionally. It will be important for both parties to work together to solve the issues — make it clear that you are an ally and you trust the school will act in the same manner as well
- **Seek professional help (if appropriate)**
Seek professional counselling for your child as necessary.

If the picture(s)/video(s) of your child resurfaces at any point in the future and/or if your child is mistreated by peers, consult with the school. Depending upon the circumstances, a school response may need to be escalated to some form of law enforcement intervention.



- **Managing peers' reactions/bullying**

Following a self/peer exploitation incident, it is important that you monitor interactions between your child and her/his peers. As a result of the incident, s/he may be targeted by peers and subjected to verbal and, in some cases, physical bullying, harassment, alienation and/or cyberbullying. This can leave your child feeling isolated, ashamed and helpless. Feelings of self-blame, guilt and humiliation may also be intensified.

Take any threat of suicide seriously and immediately seek professional help.

TOOLS, RESOURCES & GAMES FOR TEACHING ONLINE SAFETY SKILLS





Workbooks and Curriculums

- [Allconnect Internet Safety Workbook](#): A visual workbook to help guide the conversation about safety risks and rules to follow to keep children safe while online.
-  [Cyber Disclosure for Youth with Disabilities \(youth.gov\)](#): This document is a supplement to The 411 on **Disability** Disclosure: A Workbook for Youth with **Disabilities**, which helps youth learn about **disability** disclosure and what it means for them. Since that workbook was developed in 2005, there have been many advances in technology that have changed what youth need to know about **disability** disclosure. Search sites like Google, social networking sites like Facebook, and micro-blogging sites like Twitter have added a new element to disclosure. Now it is possible to disclose your **disability** on the internet without even being aware of it. This can be as simple as a picture of you using a wheelchair, a comment on your friend's blog about **disability**, or your profile posted on a **disability** organization's website. This document provides activities, examples, and key lessons to help you get informed about making and managing your own **disability** disclosure online.
-  [Safer Dating for Youth on the Autism Spectrum](#): This curriculum was authored via a collaborative process with multiple rounds of feedback from **autistic** youth, **autistic** adults, parents of **autistic** youth, and professionals and advocates who work with the families of **autistic** youth. It is intended to be used with teenagers ages 15-19 years old with a diagnosis of **ASD**, who are verbal and would like to date in the near future.
- [What's the Deal Workbook](#): This resource is used to teach youth the difference between healthy and unhealthy relationships, how to set personal boundaries, and what to do when boundaries are broken. It also touches on how easy it is to lose control of photos/ videos shared online and how to get help, if the youth falls victim to this situation.
- [It is a big deal Workbook](#): This activity book builds teen's safety confidence to help reduce their vulnerability to victimization through learning about sexual content, love vs control in dating relationships, and how to find help if they find themselves in an uncomfortable situation.

Tools and Resources

- [Cyber Safety Resource Collection \(ASERT\)](#): The internet is an important resource for learning, communicating, and socializing. However, there can be challenges to staying safe online, and it is important to protect yourself to prevent negative experiences. This resource collection

provides resources to help prepare individuals for how to stay safe online, and what to do if you have a negative experience.

- [Online Safety Tips and Tools \(ASERT\)](#): Resources developed by ASERT, that provides online safety specific information about the risks and benefits, privacy settings and social networking.
- [How to Find Someone to Date \(ASERT\)](#): When you want to start dating, it can be difficult to know exactly where to find people to date. This resource shares tips and ideas on the most common places to find someone to date.
-  [Online Readiness Checklist \(ASERT\)](#): The purpose of this checklist is for supporters to plan for **autistic** individuals who are participating in online communities so they can be as safe and prepared as possible.
-  [Cyberbullying \(ASERT\)](#): Bullying, including cyberbullying, is a serious problem that impacts many children but is even more prevalent for children who have **disabilities**. This resource provides information from various sources about bullying, how to prevent it from occurring, and what can be done to support individuals who have experienced bullying.
-  [Supporting a Safe Behavior \(ASERT\)](#): This resource, developed by ASERT, provides information for direct support staff on how to support individuals with **autism** who may engage in challenging behavior and ways that support staff can help keep everyone safe.
-  [Internet Safety for Teens with Autism \(CSESA\)](#): We live in a digital world where communication via the internet is the norm. Friends are made and maintained virtually on sites like Facebook, Twitter, Instagram, and Snapchat. Social media may be an accessible venue for adolescents with **autism** spectrum disorder (**ASD**) to build and maintain social relationships, as well as learn new things and explore their interests. While there are many benefits to using the internet, there are also risks and with easy access to the internet, teens with **ASD** must learn about these risks and how to protect themselves.
- [EE PhoneSmart License](#): EE and Internet Matters believe every child should be safe on their phone which is why we collaborated to create this free online program that provides young people with the tools and confidence to use phone technology safely and responsible
- Social Stories
 - [Online Safety Social Story \(ASERT\)](#)
 - [Online Dating Social Story \(ASERT\)](#)
 - [Online Scams Social Story \(ASERT\)](#)
 - [Romantic Scams Social Story \(ASERT\)](#)
 - [Computer Viruses Social Story \(ASERT\)](#)
 - [Social Networking Social Story \(Wordpress\)](#)
- [Safe Search for Kids](#): Safe and Secure Internet Browsing.

- [Social Media Profile Tips](#): Get tips to help your child create a good social media presence online that will help them build a good digital footprint and serve them for years to come.
- [Play Like Share films](#): Includes 3 animated videos exploring how to safely gaming sharing and social media. This includes and resource pack for professionals; additional activities and lesson plans.
- [Teens and Online Dating Guide- Advice and Support for Parents](#): Take a look at our guide to discover parental advice on helping teens make safer choices when it comes to dating online.
- [ConsumerNotice.org: Internet Safety for Kids](#): Internet safety for kids depends on parents being aware of online risks and understanding how to help their children and teens avoid them.
- [Trauma and Youth who have Experienced Online Exploitation](#): To help a child feel supported and safe, it is important for teachers and other safe adults to understand issues related to trauma and how to shape their responses toward youth. This guide contains considerations for adults dealing with youth who have experienced traumatic stress as a result of online exploitation.
- [Online Critical Thinking Guide](#): Get tips to empower children to make smarter informed choices to navigate their online world safely.
- [Digital Resilience Toolkit](#): Give your child a guiding hand as they start their digital journey online with practical tips to help them build up their understanding of the online world and create a safe space for them to explore.
- [Understanding and Combatting Youth Experiences of Image-Based Sexual Harassment and Abuse](#): These resources from the Association of School and College Leaders (ASCL) follow their research into image-based sexual harassment and abuse. These workshops around the issue aim to help teachers inform and educate students.
- [TikTok Playbook](#): With a whole world of digital content at your students’ fingertips our TikTok Playbook has all the information and advice you need to recognize the potential safeguarding issues understand the latest privacy and security features and support students to use the platform safely.

Games

- [Find the Fake](#): A fun interactive quiz to help families learn to identify “the fakes” online.
- [Don’t get sextorted, send a naked mole rat](#): Not only educated teens and tweens about what sexual distortion is and how it can happen, but also provides a unique way to prevent it.
- [Zoe and Molly Online](#): This interactive series gives kids an opportunity to have fun exploring what it means to be safe while playing games online using comics, quizzes and more.

- [BBC Bitesize](#): An interactive video that helps children to recognize and avoid potentially dangerous situations online.
- [The Digitally Smart Guide — LEGO](#): LEGO has released a series of online guides to help you and your child live digitally smart lives.
- [Online quiz about staying safe online](#): Created by O2 and NSPCC the online quiz about staying safe online aim to get the whole family together in this game between parents and kids.
- [Digital Matters learning platform](#): Created with support from ESET Digital Matters is our new learning platform to help schools change the way they teach online safety. With interactive activities discussion and immersive scenarios kids will get excited about digital safety.