The Kingston Interval House

# INTERNET SAFETY AND SECURITY

How to Stay Safe Online in 2021+

## Introduction

It is important to recognize how it is not the app or the social network itself that raises issues of danger online, but rather, it is how people interact with the app or the social network that makes it dangerous. Social networks, websites, apps, and video games; we constantly hear about their negative effects and their associated risks for danger, however, we rarely are informed about how to prevent these dangers.

Moreover, we hardly hear about the incredible benefits of these online tools and platforms. For instance, Professor Shapiro of Temple University stated in 2019 that:

> "Kids aren't losing themselves in their devices but potentially finding themselves. What's more, they're doing exactly what generations of kids have long done by immersing themselves in the toys and objects of the moment that reflect the society they inhabit and which help them prepare them for the future."[1]

As such, this article aims to not only equip you with steps to increase your safety online, but also to inform you about the positive effects of the internet in our lives and in society as a whole. We believe that by informing ourselves about the risks and learning how to avoid them, we can begin enjoying the benefits of the internet without compromising our safety.

[1] "TikTok: Fear, Facts, And Confusion," The White Hatter, February 3, 2021, https://www.thewhitehatter.ca/post/tiktok-fear-facts-and-confusion.

### Privacy Protection: 10 Quick Tips to Remember

1. Use strong passwords, and don't use the same password or PIN number for multiple accounts and/or devices. This also applies to debit/credit cards.
2. Use two-factor authentication or password-reset checks for all your accounts.
3. Avoid using social media or email on public devices or public/shared WiFi. If you must, ensure that you log out afterwards and delete your browsing history.
4. Make your accounts private if you do not want strangers to find your profiles and shared information.
5. Disable access to geolocation data for your social media apps.
6. Be wary about clicking links from friends in social media; you never know if they've been hacked. If something looks suspicious or does not sound right, it likely isn't.
7. Even on your private social profiles, keep personal information to a minimum. For example, limit your work history, addresses, education, recent locations, etc.
8. Use "private browsers" or "incognito windows" when using the internet to avoid your history being saved. If you do not use private browsers, ensure you are frequently clearing your history and your caches. Click here to follow steps for how to clear your cache. If you do use private mode, still be mindful of the information you share as this cannot guarantee your safety.
9. Never share your information over emails or phone calls unless you are 100% positive and can verify that the provider is legitimate. It is important to know that legitimate services will never collect detailed personal information like a SIN number via email.
10. Report all inappropriate and suspicious behaviour whenever possible, including fraudulent emails, phone calls, and SMS messages.

## Online Apps and Social Networks

The massive influx of personal information that has become available and stored online raises concerns for many users in regard to their safety. A series of issues have been identified relating to privacy of information in the online environment. Among these issues, arguably the most important are: follow up and monitoring the internet users' activity, gathering and analyzing information, taking personal information out of their context, and collecting users' data.[2]

We have provided hyperlinks to an informative website that provides information about each of the most popular online apps and social networks in specific detail. This resource, eSafety, will explain to you what the social network or app is, what it is used for, how it can be used with other elements, how you can report abuse or violations within the network or app, how you can protect your personal information and security, and key safety links including terms of service

[2] Mircea Turculet, "Ethical Issues Concerning Online Social Networks," Science Direct, Stefan cel Mare University, October 5, 2014, https://reader.elsevier.com/reader/sd/pii/S1877042814050307?token=3444F2D4BDD8E95EBBE2F8E68CADBF64224D95464B4903BA4D517D3288CA405ED445775689DB73E10BA0FABE4A4BACC4, 969.

and help centre. Throughout each page associated with each network or app, you will find several hyperlinks including important things such as where to go to report abuse or inappropriate activity and the official privacy policy.

Disclosure: eSafety is a legitimate, independent statutory office supported by the Australian Communications and Media Authority, who has formed a website designed with the commitment to helping internet users stay safer online.

**Social Networks:**

1. Zoom: eSafety Guide to Zoom
2. Houseparty: eSafety Guide to Houseparty
3. Omegle: eSafety Guide to Omegle (See Warning)
4. Roblox: eSafety Guide to Roblox
5. Onlyfans: eSafety Guide to Onlyfans
6. Seeking Arrangements:
7. Chatruletka

**Apps/Social Media:** Note that steps can be taken to make your accounts and information private.

1. Tik Tok: eSafety Guide to TikTok
2. Snapchat: eSafety Guide to Snapchat
3. Instagram: eSafety Guide to Instagram
4. Facebook: eSafety Guide to Instagram
5. Twitter: eSafety Guide to Twitter
6. YouTube: eSafety Guide to YouTube
7. Tinder: eSafety Guide to Tinder
8. Bumble: eSafety Guide to Bumble

## Additional Information

We have provided additional information about potential risks and safety concerns for social networks and apps below. Please note that this additional information is no longer in relation to or affiliated with eSafety.gov.au. We also provide the positive experiences and testimonies that people enjoy whilst using these social networks and/or apps. We encourage that users become aware of the safety risks and take steps to overcome them in order to enjoy the great benefits from these online experiences.

For instance, you may be shocked to realize: Who Owns Photos and Videos Posted on Facebook, Instagram or Twitter? Once you post on these sites, that although you still own the photograph, you grant the social media sites a license to use your photograph any way that they see fit for free and you grant them the right to let others use your pictures/videos as well.

**TikTok**

We'll start by talking about arguably the most popular social media app in 2021. Tik Tok has definitely received a negative reputation at times, but are the rumours true? Let's find out.

An excellent website to begin with reading is TikTok: Fear, Facts, And Confusion. This site, The White Hatter, does an excellent job explaining what is true and what is not. When you click the hyperlink, you will see how they format this page by stating the concern and then telling you if it is true or misinformation. Additionally, the website helps you understand how to protect yourself from any risks.

Another informative website to read is Does TikTok Own My Content & Videos? (Basic facts) – Mangoful. This link will take you to a site which explains in depth about *who* owns the content and videos that you post on Tik Tok. There was buzz going around over the past year about Tik Tok owning your videos. Take a read to understand the truths and the rumours. A major takeaway to understand is that much of your privacy concerns can be resolved in the settings and control options. For example, you must turn off the download options for your videos if you do not want people able to download them. This step is very simple. You also have the option to make your account private. Another simple step.

I have taken out one of the most important statements from The White Hatter's webpage: People believe that TikTok is currently collecting my personal information and selling it to third parties. In Tik Tok's privacy policy, they clearly state that they do not sell personal information to third parties. However, they may provide your private information and meta-data to "Service Providers and Business Partners" to help them perform business operations.[3]
It is important to remember that any app that is free has to earn an income to sustain its business model which TikTok does through its advertisers much like every other free app on the market. There is just no credible evidence that we could find to support that TikTok presently sends any data to China, and there is no solid proof that any information is pulled from users' devices over and above the prying data grabs typical of all social media platforms.

People believe that it has a lack of parental controls and privacy protection but that could not be more untrue. Since late 2020, TikTok is the only app, of the top 4 apps that are most popular with youth (TikTok, Snapchat, Instagram, YouTube), to actually have parental controls that cannot be turned off by the youth via the TikTok "Family Pairing Function." Also, TikTok is the only app that if a youth joins TikTok, and is under the age of 16, their account is:

a) Automatically set to private – which the youth can't change
b) They can't receive or send direct messages
c) They can't download videos

[3] The White Hatter, "TikTok: Fear, Facts, And Confusion," The White Hatter, February 3, 2021, https://www.thewhitehatter.ca/post/tiktok-fear-facts-and-confusion.

d) They won't receive messages from people who are not following them
e) Tighter restrictions on comments that parents can control
f) Access to the "Duet" and "Stitch" function will only be available to those over the age of 16yrs. For those between the ages of 16-17 years, the default setting will be "friends" only
g) If the child attempts to opt-out of Family Pairing, a parent will be immediately notified via their Family Pairing

Ultimately, so many youth and even adults have vouched that they established their identity and made connections with so many individuals on this site. There is a ton of information available on this app that serves as educational. Like most apps, this one is all about how you use it - it will put certain videos on your FYP based on the videos you seem to be liking/following the most. There are plenty of parental control options and even time limits that you can put on for yourself to make your experience with Tik Tok as positive as possible.

**Tinder**

tinder

The main thing while using Tinder is to be safe and use good judgement. The app does not perform background checks or vet any of their uses so you need to be vigilant while using the app. Warnings and safety risks to be aware of while using Tinder include:

a) Predators and sex traffickers often look for teens on Tinder.
b) Pictures that the user posts on their profile or sends in messages to their matches can often reveal their exact location.
c) Scammers use Tinder (note that this is common for most social media sites and not just specific to Tinder).
d) In-person meetings can be dangerous. To avoid this danger, ensure that you meet somewhere public, safe, and even have a friend drop you off and stick around the area until you give them the signal that you feel safe.

Positives of Tinder:

a) Plenty of successful relationships and marriages have been formed.
b) It is an excellent way to "meet people" in 2021 when social lives and dating have been extremely limited due to COVID-19. This has opened a lot of doors for new relationships in a very difficult time.
c) Prevents loneliness and even leads to friendships.

While you cannot control the actions of others, there are things you can do to help you stay safe during your online dating experience. This advice is taken directly from Tinder's website and policies: [Safety | Tinder | Match. Chat. Meet. Modern Dating]

Tinder's Dating Safety Tips (please click the hyperlink above so that you can see all of these tips in much more detail and with explanations on the website).

a) Never send money or share financial information.

b) Protect your personal information.
c) Stay on the platform.
d) Be wary of long distance and overseas relationships.
e) Report all suspicious and offensive behaviour.
f) Protect your account.

Tinder takes these "Dating Safety Tips" to the next level by providing, "Meeting in Person Guidelines" and "Sexual Health and Consent." They even provide "Resources for Help, Support or Advice" all within the same link click here and scroll down to read more.

As you may already know, there are several different online dating apps and websites including Hinge, Match, Plenty of Fish, Bumble, and OKCupid. Each of these apps has their own website similar to Tinder which provides details about safe dating advice.

An example of another extremely popular dating app is **Hinge.** While the risks to dating are reciprocal to Tinder, the benefits are likewise the same. You can click Safe Dating Advice – Hinge to see the parallels in advice. However, it is vital to understand that each app or website has its own privacy policies and it is important that you make yourself aware of how you can protect yourself while using them.

Here is a video Online Romance Imposter Scams | Federal Trade Commission that explains the risk of romantic imposter scams online. You can find several other informative videos on YouTube about scams and/or online safety, particularly with online dating. Another helpful tip is to read case studies about experiences people have had with online dating in order to understand how to protect yourself. However, if you choose to do this, we also encourage that you watch or read testimonials from individuals who have had excellent success with online dating. Again, we remind you that it is important to know the risks with using tools online, but also equally important to understand the benefits. By informing yourself, you can safely use these apps and social networks.

## Instagram

Instagram allows you to follow accounts that align with your interests and, if you choose, to maintain your own profile that presents yourself to your followers, friends, and sometimes even the world.[4] Similar to most areas of the internet, depending on whom you follow or what you search for, you can find lots of positive content. Likewise, you can find lots of negative content. With some guidance around settings, limits on use, and ongoing conversations about content and comments, Instagram can be a place for everyone, including kids, to connect and be creative.[5]

[4] Christine Elgersma, "Parents' Ultimate Guide to Instagram," Common Sense Media: Ratings, Reviews, and Advice, March 10, 2021, https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-instagram.

[5] Christine Elgersma.

Let's talk about some concerns with who can view, and even who owns the photographs you post on Instagram. If you do not want to have your photos seen publicly, we recommend the easy switch to make your account private. This forces people to request to follow your account and wait for your approval. It is important to note that when you post an image on Instagram, according to their policy, your photos can be used by others in any way that they want. You grant the social media site a license to use your photograph anyway they see fit and you grant them the right to let others use your picture as well unless you have a patent or copyright on your photo. While it is rare that others will "use" your photos, do also consider that anyone can even simply screenshot and save this photo to their own device. So, again, just be mindful of what you post on your social media to stay as safe as possible. Familiarize yourself with the Terms of Use | Instagram Help Center and Safety Tips | Instagram Help Center.

One other thing to consider while using Instagram is your location. Instagram not only tracks your location given your permission, but you should think about the photos you post regarding the background. If you are concerned about your privacy, consider who is following you, what your privacy settings are, and how much your photographs give away your specific location.

Now let's discuss the DM function on Instagram. Similar to Facebook, you can choose to turn off the DM function to anybody who is not following you. This can be updated in your Account Settings; Click here for a guide to Where are my Instagram account settings?

If you happen to leave this DM function open to the public, or have your messages go to message requests, this can lead to messages from people you do not know. For instance, many young people have experienced older men/women messaging and offering them money in exchange for some kind of personal service, otherwise and commonly known as a Sugar Daddy or Sugar Mamma. This can potentially lead to some major risks. While this is not common for everybody, just be aware of the possibilities and signs. If you choose to engage in this kind of service, ensure that you educate yourself about how to stay safe. A safer approach is through services like Seeking: Online Dating for Successful & Attractive People where you are more protected by the contract that you create and you personalize your level of comfortability. To learn more about sugaring and teen vulnerability, we suggest reading A True Story of Teen Vulnerability: The Online Sex Industry and The Lure of Easy Money.

Learning about your safety while using Instagram allows you to stay creative and stay safe. Enjoy your creative expression on the app, and keep sharing what you love! Just be mindful.

**Snapchat**

Snapchat can be a wonderful way to stay in touch with friends and family, particularly during COVID-19 when we are missing our loved ones. It provides us a way to stay connected on a more personal level by chatting through photographs and texts. It is important to ensure that you monitor the friends that you have on this app for this reason.

Snapchat provides a detailed guide to their Privacy Settings and how you can take steps to make your information more secure. This page explains your privacy settings options, from who can contact you, send you notifications, view your story, to who can see your location and search for your username to add you as a contact. This page also guides you about how and where to change your privacy settings. Moreover, the page explains a lovely list of tips under “A few things to remember.” If you need any further assistance, you can select “YES” when they ask “Need help with something else?” which takes you to the option to contact Snapchat about reporting a safety concern and asking a privacy question to them directly.

Some key tips include to remember to turn off your snapchat location tracking unless you trust your friends in the app and do not mind them seeing your whereabouts at all times. This detail in Snapchat even shows your friends when you are driving or on the move, so just remember if you choose to turn it on that it can be turned off. If you are experiencing any inappropriate behaviour please visit Report Abuse on Snapchat for guided steps for reporting. Additionally, if you are experiencing sextortion, report this to Snapchat if you are comfortable, but please see more detailed information about steps to take under “Only Fans” in this article where explicit guidance is provided. Since Snapchat is a place for photos to be shared with others, there is always the potential risk for image-based abuse.

**Facebook**

Like any social media or social network, Facebook’s terms and conditions are subject to change at any time. This means it is important to continuously check for changes. Often, apps or social networks will inform you with a notification or pop-up that their terms and conditions have been updated. The typical reaction is to disregard or ignore this notification, but it is crucial that we at least understand what policies cover our safety while using the social network. With this being said, under Facebook’s current terms, by posting your images and videos, you grant Facebook “a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any [IP] content that you post on or in connection with Facebook (“IP License”).” This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.  Beware of the words, *transferable, sub-licensable, royalty-free, worldwide license*.  This means that Facebook can license your content to others **for free** without obtaining any other approval from you.

Perhaps most important of all is to be aware that once your photos or videos are shared on Facebook, it could be impossible to delete them from the public viewing, even if you delete the content or cancel your account. Not only is the content still existent in Facebook servers, but anyone from your friend list, or public, depending on your privacy settings, can save your images to their own devices. To avoid this from happening, ensure that your privacy settings are set to the strongest possible, and of course be mindful of the things that you share and post.

Additionally, you may have noticed that when you use other applications with your Facebook account, those applications have their own terms and conditions and often ask for your consent to share all your profile information with that app. Typically, users just click yes without actually reading what this entails. We encourage you to always read the fine print to ensure you are not agreeing to something that you do not want.

Facebook is a wonderful way to stay connected with friends and family globally, particularly in such unprecedented times during 2021. However, in order to ensure that your privacy is top notch while using this social network, here are some suggestions for you:

a) Go to settings & privacy. Then select privacy.
b) Here, you can change things like "who can see the people, pages, and lists you follow." If you want, you can change this to 'friends' or 'only me.' This keeps your interests private.
c) If you are concerned about people sending friend requests or searching for your profile, you can change the settings for "how people can find and contact you." You can likewise, under this heading, edit who can see your friends list, who can look you up using the email address you provided, who can look you up using the phone number you provided, and whether you want search engines outside of Facebook to link to your Profile.
d) Below this same heading, you can also edit who can send you chat messages or chat requests. We suggest selecting the option "don't receive requests" for all of the prompts if you wish to remain as private as possible to anyone who are not your friends on Facebook.

The best privacy tool to use on Facebook when looking into your privacy settings is the "view as" option. This allows you to review what the public sees on your profile when they search for you (those who are not your friends). If you notice that they can see anything you want to be kept private, edit your profile details and your settings to ensure you are protected. This also helps keep your personal life private from employers, for instance. But, like we said, anything you post can be saved by others or out on the internet forever, so ensure you only post what you are comfortable having others see.

## Twitter

The following information is taken directly from Twitter Terms of Service:

> "By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods now known or later developed (for clarity,

> these rights include, for example, curating, transforming, and translating). This license authorizes us to make your Content available to the rest of the world and to let others do the same. You agree that this license includes the right for Twitter to provide, promote, and improve the Services and to make Content submitted to or through the Services available to other companies, organizations or individuals for the syndication, broadcast, distribution, Retweet, promotion or publication of such Content on other media and services, subject to our terms and conditions for such Content use. Such additional uses by Twitter, or other companies, organizations or individuals, is made with no compensation paid to you with respect to the Content that you submit, post, transmit or otherwise make available through the Services as the use of the Services by you is hereby agreed as being sufficient compensation for the Content and grant of rights herein."

Similar to Facebook's privacy concerns with what is posted and saved on the internet, Twitter outright states that you grant them the rights to use your content and make it available to the rest of the world. Just be aware of these things! It says it right in the privacy policy that you agree to when settings up your account. If you do not agree to the terms and services, you are prohibited from creating an account.

Similar again to Facebook, take precaution with your account settings Account Settings - Twitter by making your information private. You can make your account private, limit who searches for your username, make your tweets unable to be retweeted or reshared and more.

**Only Fans**

An interesting and informative read that we suggest for you is, How COVID-19 Has Spawned the Rise of the App OnlyFans. While Only Fans can be safe depending on how it is used, there are cases where users have been extorted for example a client was able to find the user's real name, address, and social networks - they threatened to publicly post screenshots and recordings of what the owner was doing to their friends and family if they did not begin to provide free content or meet with them face-to-face. It must be emphasized that anything and everything done on an Only Fans page can be covertly recorded without the owner of the page knowing.

Concerns with Only Fans also include sextortion. "Sextortion is a form of blackmail where someone threatens to share intimate images of you unless you give in to their demands."[6] Sextortion: eSafety Commissioner provides information about the warning signs of sextortion and more.

Let's talk about image-based abuse for a minute. The non-consensual distribution of intimate images (including videos) can occur in various situations, including relationship breakdowns,

[6] "Sextortion," eSafety Commissioner, n.d., https://www.esafety.gov.au/key-issues/staying-safe/sextortion.

cyberbullying, and blackmail on social apps.[7] The YWCA Canada is a leading voice for women, girls, Two-Spirit and gender diverse individuals; as such, they have provided a quick guide on sexual image based abuse. This webpage they created provides information about rights, reports, and supports. For instance, a key message within this webpage states that, "you are not to blame if someone is in any way abusive or disrespects your rights."[8]

If you are victim to sextortion and are unsure what steps to take, eSafety outlines the following steps for Canadians:

1. Report Sextortion to one of the following:
   a) NeedHelpNow.ca - Helps teens in Canada stop the spread of sexual pictures or videos and provides support along the way.
   b) Project Shift - A project funded by Status of Women Canada, YWCA Canada and partners, who are working to create a safer digital world for girls and young women.
   c) The Canadian Centre for Child Protection - Operates Cybertip.ca, Canada's tipline for reporting the online sexual exploitation of children, and includes information and support for victims of image-based abuse.
   d) The Cybersmile Foundation - A multi-award winning anti-cyberbullying non-profit organisation, committed to tackling all forms of digital abuse and bullying online.

Additionally, if you are looking for some support, here are some helpful links: **badassarmy.org**, **draw-the-line.ca**, and **Techwithoutviolence.ca**.

### YouTube

Youtube is a phenomenal education tool. Teachers even use this on the daily to show their students videos about certain subjects or topics.

But, like anything, there are privacy risks and concerns. For starters, for many apps and games it is easy to lie about your age. This is applicable to YouTube when watching censored videos. Although YouTube tries to censor these videos, it is too easy for children to simply click that they are of age before watching explicit content. A way around this is for parents to place restrictions by creating a YouTube family account - you can find more information about this by visiting the following link: Set up & manage a YouTube family plan - Android - YouTube Help.

Additionally, by going to the profile icon in the top right corner, on both the desktop and the app, you can easily go to settings and make adjustments for your account. You can select "Privacy" along the tab options which gives you the options to:

a) Playlists and subscriptions - you have the option to "keep all my saved playlists

[7] "A Quick Guide on Sexual Image Based Abuse," YWCA, n.d., https://ywcacanada.ca/guide-on-sexual-image-based-abuse/.
[8] YWCA.

private” and “keep all my subscriptions private”

b) It also provides information about ads on YouTube, explaining how the ads you see also depends on your Google Ads settings (https://adssettings.google.com/authenticated?hl=en) here you can turn off ad personalization. This stops Google from gathering information to provide personalized ads.

c) There is also a hyperlink for https://support.google.com/families/answer/7087279?hl=en which explains ads and Google Accounts managed with Family Link.

Unfortunately, in 2019 U.S. based Google and YouTube (since Google owns YouTube) were fined $170 million dollars for knowingly and illegally harvesting personal information from children and using it to profit by targeting these youth with ads.[9] Ads can be annoying, sure, but it is important that we understand that the ads are the highest source of income from YouTubers who make these videos for a living. To ensure your protection from receiving personalized ads, however, turn off Ad Personalization by visiting the following link Google Account.

**Find My Friends**

Follow this link to read and understand how and why the app Find My Friends is used on iPhone and other Apple devices: Set up and use Find My Friends in iOS 12 or earlier.

There are always concerns about your device tracking your whereabouts. Since that is quite literally the purpose of this app, ensure to remove contacts who you no longer want tracking your whereabouts and opt to hide your location if you are ever not wanting to be tracked.

## Video Games

One of academia’s most prestigious science journals just gifted video game enthusiasts with this unusually awesome opening paragraph: “Playing action video games substantially improves performance in a range of attentional, perceptual, and cognitive tasks,” writes a research team in the November issue of the *Proceedings of the National Academy of Sciences*.[10] Those playing the fast-paced shooting performed better at a visual perception task, which the researchers suspect have benefits to real-world learning. Previous research on video games shows that enhanced visual training improves the skills necessary to be a good surgeon or pilot. This particular study

[9] The White Hatter. “TikTok: Fear, Facts, And Confusion.” The White Hatter, February 3, 2021. https://www.thewhitehatter.ca/post/tiktok-fear-facts-and-confusion.

[10] “Playing Action Video Games Can Boost Learning, Study Finds,” ScienceDaily, November 10, 2014, https://www.sciencedaily.com/releases/2014/11/141110161036.htm.

also found that the benefits to fast-paced video games lasted at least several months to a year after training, proving that Call of Duty and others can have long-term benefits.[11]

We have again provided hyperlinks to eSafety which explains what the video game is, how people use it, how you can report abuse or violations with the video game, how you can protect your personal information, and also provides key safety links including the support centre, community code of conduct, and terms of use.

Disclosure: eSafety is a legitimate, independent statutory office supported by the Australian Communications and Media Authority, who has formed a website designed with the commitment to helping internet users stay safer online.

1. Call of Duty: eSafety Guide to Call of Duty
2. Among Us: eSafety Guide to Among Us
3. League of Legends: eSafety Guide to League of Legends
4. Fortnite Battle Royale: eSafety Guide to Fortnite Battle Royale
5. Apex Legends: eSafety Guide to Apex Legends
6. Minecraft: eSafety Guide to Minecraft
7. NBA2K20: eSafety Guide to NBA2K  (and other EA games like NHL, Madden, etc.)

## Additional Information

### Among Us

The game collects data driven by Google in order to serve up ads when you are on the free version of the game. There is a disclaimer you will see when setting up the app. You have the option to remove ads by upgrading to the paid version, or you have the option to actually see "What is Collected?" which is nice for parents. If the ads make you nervous, you can upgrade for $2. The game allows players to connect with other players **from anywhere** which of course brings inherent stranger risk that any online game has. The game also has **in-game chatting** which can be censored in the settings (to censor out curse words for example) but it still allows the risk for online strangers.

### Apex Legends

Every player is on a team of three, so unless you or your child has two other friends with the same gaming platform, they will be playing with people that they don't know. This carries the

[11] Science Daily.

risk for exposure to predators. It is possible to play the game safely (the game is not recommended for kids under 14) with the right chat settings and parental guidance. The safest way to play is on a squad only with people you know or to mute voice and text chat.

**Fortnite**

Fortnite is fairly safe as video games go, and the violence feels more cartoon-like than others like Call of Duty. You may begin the game with 100 players, but do not fret because you cannot actually communicate with all of them. You can only communicate with the players in your party. You can choose to have only friends in your party (you can choose 1s, 2s, or 4s where you can choose to play alone in the party, join with a friend, or join with three players). If you or your child is unable to play with friends, you can alter your privacy settings so that you do not *have* to chat with the other players. How do I change the settings for voice chat in Fortnite? - Fortnite Support. We also encourage that you read through the Privacy Policy for more information.

**Call of Duty**

Frequent concerns with the game include the voice chat and online play chat. Not only does this create the obvious atmosphere of aggression and violence, but it also sets the risk for communicating with strangers.

A major issue with the game is that there is no single way to report abusive behaviour in games in the Call of Duty franchise, however, you can report a player by following the hyperlink which provides instructions on how to report someone who is being offensive or abusive in Call of Duty: Modern Warfare.

It is important to know that you can protect your information by visiting the Online Safety Guide. Here you can explore Activision's online safety guide for Call of Duty to learn how to make your account and gaming experience as secure as possible. In addition, the Privacy Policy outlines in detail how Activision collects, stores, and uses your information.[12]

*General ways that your privacy might be at risk while playing video games include:*

1. Camera and microphone access - many multiplayer games require the microphone access to communicate. Younger children in particular might not realize that the

[12] "Call of Duty," eSafety Commissioner, n.d., https://www.esafety.gov.au/key-issues/esafety-guide/call-of-duty.

microphone is picking up everything that they say. If someone happens to be speaking about personal information in the room, that would be transmitted to whoever was listening.

2. Location tracking - Some games like *Pokemon Go*, track your real-world location and sometimes sell this information to advertisers. If you go to a store a lot and your game location settings notices this, it can tell the advertiser to start showing you ads for products like what is being sold in that store. This is invasive enough without your consent, but it would be even more harmful if this same data was revealed by a security breach. You can mitigate both these issues by turning location tracking off when not playing, if possible.
3. Poorly protected server. Hackers can breach any company's servers without you making any mistakes on your own, which is why it is important to limit the information you share online and familiarize yourself with the track record of companies that store your information. Perhaps the most infamous example of this was the Sony PlayStation hack, when hackers breached the company's database and got access to the personal information of over 70 million user accounts including names, passwords, credit card details, and addresses.
4. Online gaming malware,"malicious code," can be inserted into the game itself especially if it has been pirated. This code is used to access your personal information, such as login details, passwords or even payment information. Beware of free games from unknown developers.

Protonvpn.com: The good news is that if you take online gaming privacy seriously, there are many things you can do to stay safe. You can follow them on social media to stay up to date on the latest ProtonVPN releases: Twitter | Facebook | Reddit | Instagram. To get a free ProtonMail encrypted email account, visit: protonmail.com.

## Website Browsers and Phones

While we may think that most of our privacy risks come from the apps and social networks we use, it can be shocking to discover the risks that are simply within the browsers we use and even our cellphones in general.

There are several settings that come turned on when we first begin using a new phone. We encourage you to browse through your Privacy Settings to see what is turned on and what you would prefer turned off (just an extra tip, this likewise applies to your data roaming on your apps and if you do not want to have them constantly running all the time in the background you should turn them off too). Key things to look for in your Privacy Settings include Location Services, Tracking, Contacts, Photos, Microphone, Camera, and Research Sensor & Usage Data.

For those of us with iPhones, there are more specific things to look for that are turned on in your phone including, **"Significant Location Services"** that may surprise you. Have you ever noticed that your iPhone sends you messages from your map app like, “only 10 minutes from home” when you do not ask it to do this? Or, “only 20 minutes to Mom’s house.” This is because you have the “significant location services” turned on - iPhones typically come with this service on now with the newest updates. If you want to turn this off, take the following steps:

Settings → Privacy → Location Services → System Services → (scroll all the way down) Significant Locations (click, insert password) → View all the history to see the creepiness factor, then turn Significant Locations off. Be mindful that the intention of Significant Services is to make your life easier with map suggestions, not to creep you out. This is a personal preference if you choose to leave it on or not.

While using web browsers there are various steps to protection including browsing in incognito or private windows and frequently deleting your history and cache. The settings for each browser (Safari, Chrome, Internet Explorer, Firefox, etc.) all vary. Additionally, the settings for each search engine varies (Google, MSN, Bing, Outlook, etc.). We will provide some information about Google below to give an example, but we do encourage you to do some research and some digging about your preferred search engine’s privacy settings.

A common question people ask is: What are computer cookies? Click this link to gain a better understanding of your safety while using the internet. This site explains to you when you should keep your cookies to yourself and when they are and are not safe.

**Google**

By following this hyperlink, Manage your Google Account, you will be taken to the various options for your privacy and security settings.

a) You can manage your info, privacy, and security to make Google work better for you.
b) Most settings will be automatically turned on. So, this page allows you to navigate your settings in order to turn them off.
c) To turn off personalization in your google account you select “Privacy & Personalization” … you can go through the privacy suggestions, ensure that your settings are all turned off - particularly the location history.

**Google Home, Amazon Alexa, etc.**

Ensure that your home devices are secure. Home devices refers to any devices in your house that are controlled by WiFi. The most popular are Google Home’s Assistant and Amazon Alexa. You can find more information by visiting these links directly:

a) Choose what to share with your Google Assistant - Google Assistant Help
b) Amazon.ca Help: Manage Your Alexa Privacy Settings

Again, ensure that you do not give these network passwords or controls to anybody else. Double check that your privacy settings are up to date the way that you prefer them to be. If you were living with someone who had access to these controls, you can take them off of this by changing the password and/or settings for who can manage the devices.

## Conclusion

Overall, let us remind you that our purpose here is not to scare you from using technology. Our new world is driven by technology, and using it actually brings us more benefits than risks. We simply believe that if we can be informed about these risks and potential dangers while online, we can feel equipped and confident about protecting our safety. The harsh reality with online chats is that the predators are always going to be where the kids are online, and all online chats struggle with content being shared regardless of how good their syntax controls are. Several solutions to solving the issue of privacy in the online world have been brought forward in this article and beyond. The first step to keeping ourselves safe is to remain educated about what the potential threats are and how we can avoid them.

While it is practically impossible to cover every concern out there on the internet, we hope that this article has been helpful to aid your understanding about how to stay safer while using apps, personal tech and social networks.

**10+ Helpful Websites Links for Additional Information**

*Each of these links will take you to informative websites which have plenty of opportunities for further reading beyond the following ones we suggest.*

1. Kids' Safety Online
2. READ: Internet Safety Resources, Guides and Tips for Everyone
3. The eSafety Guide
4. 10 Reasons Why Minecraft Is Beneficial For Your Kids
5. Online scams and identity theft
6. Top five social media privacy concerns
7. See Articles: Parents' Ultimate Guide to Instagram
8. Internet Safety 101: sex trafficking
9. Top Websites to Teach Kids About Internet and Cyber Security
10. Among Us App Review. Is it safe? What's the buzz?

Bibliography

"A Quick Guide on Sexual Image Based Abuse." YWCA. n.d. https://ywcacanada.ca/guide-on-sexual-image-based-abuse/.

Call of Duty." eSafety Commissioner. N.d. https://www.esafety.gov.au/key-issues/esafety-guide/call-of-duty.

Elgersma, Christine. "Parents' Ultimate Guide to Instagram." Common Sense Media: Ratings, Reviews, and Advice, March 10, 2021. https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-instagram.

"Playing Action Video Games Can Boost Learning, Study Finds." ScienceDaily. November 10, 2014. https://www.sciencedaily.com/releases/2014/11/141110161036.htm.

The White Hatter. "TikTok: Fear, Facts, And Confusion." The White Hatter, February 3, 2021. https://www.thewhitehatter.ca/post/tiktok-fear-facts-and-confusion.

"TikTok: Fear, Facts, And Confusion." The White Hatter. February 3, 2021. https://www.thewhitehatter.ca/post/tiktok-fear-facts-and-confusion.

Turculet, Mircea. "Ethical Issues Concerning Online Social Networks." Science Direct. Stefan cel Mare University, October 5, 2014. https://reader.elsevier.com/reader/sd/pii/S1877042814050307?token=3444F2D4BDD8E95EBBE2F8E68CADBF64224D95464B4903BA4D517D3288CA405ED445775689DB73E10BA0FABE4A4BACC4.