Cyberspace: Not A Playground for Children

Brent Clabaugh

October 2022

University of Maryland Global Campus

Abstract

Cyberspace is no longer the internet Generation X once knew. A new generation has emerged that is far more than connected, they are immersed in the internet. Children as young as five have smart devices that connect them to the world wide web. Developers create apps aimed for children without the security of children in mind. This paper looks at the threats that target today's younger generation, what measures are being taken to mitigate cyber threats, and what actions are being taken to help parents and children protect themselves. After reviewing Apple's iOS Store and Google's Play Store policies, they do not take into consideration the threats that face children, only implementing what laws have governed them to do. How do apps with malware and viruses get submitted for approval, and so many are approved? How do apps with questionable content not get questioned by the app review boards? What are parents and children to do to protect themselves? What resources are available to them? They need help navigating the millions of apps on the market because cyberspace is not a playground for children.

Cyberspace has grown immensely in the last 30 years. An entire generation has been born and raised with the internet at their fingertips. Unlike the Earth that has had every square mile of its oceans and lands mapped out, cyberspace expands faster than can be explored. There was a time when a person could endeavor to go from one end of the internet to the other, before it became public domain. Even then, the dangers of the new frontier were rife with code that could bring ruin to those who dared to blindly venture in. In 1988, a year before the World Wide Web officially went live, a graduate student at Cornell University, Robert Tappan Morris, created experimental code that went horribly wrong. It was designed to copy itself to every system it encountered on the network and only copy itself if it were not already there. However, Morris suspected admins would kill the code, so he set it to copy itself no matter what. This flawed experiment came to be known as the Morris worm. Although it caused no loss of data, it paralyzed half the known internet (6,000 computers) and ultimately $100,000 in other damages. He was also the first to be convicted under the newly minted Computer Fraud and Abuse Act of 1986. Today he teaches at MIT and assists in cybersecurity (*The Morris worm*, 2018).

This accidental worm brought forth the nation's first Computer Emergency Response Team (CERT). Many other organizations have spawned from the demand of addressing worms, viruses, malware and more. The internet has grown to foster more than just information sharing, it now provides education, entertainment, and employment. With infrastructure built to sustain billions of users, and IPv6 able to provide thousands of IP addresses to each user, thus expanding the ability to connect the physical world to cyberspace is a reality. The Internet of Things (IoT) is an exploding market full of gadgets and everyday items that can connect to the internet and provide convenience only imagined in 1988. Today, smartphones can connect humans to the internet in ways never before conceived. Where the first generation grew up with the internt available, this 2nd generation of children are being raised fully immersed in the internet. As cyberspace exploration grows, threats increase with every piece of code written to

take advantage of it. Unfortunately, like the wild west, there are plenty of villians out there looking to take advantage. This paper looks at the threats that target today's younger generation, what measures are being taken to mitigate cyber threats, and what actions are being taken to help parents and children protect themselves.

There is a meme that succinctly portrays how internet culture has evolved and how the younger generation is threatened. It reads: "1998: Don't get in car with strangers. 2008: Don't meet people from the internet alone. 2018: UBER – Order yourself a stranger from the internet to get into a car with alone" (author unknown). The next generation of cyber criminals are not only looking at the wealthy, middle-aged folks, or corporations, all of whom could most likely afford top level cyber security. Criminal behavior, by nature is opportunistic. Cyber criminals are no different. With the proliferation of smartphones around the world, and the access that children today enjoy, cyber criminals have been targeting children as young as five years old by installing malware and spyware through apps in the Apps store that a great majority of phones utilize to browse, find and install. These malicious actors design apps with appealing colors and simple games that promise to entertain and attract children (Henry, 2018). In 2018, University of Michigan (Development and Behavioral Pediatrics Dept) conducted a study which found that 95% of most popular apps downloaded for kids actually target kids 5 and under while carrying the label of being educational. The study stated the ads are "deceptive"," manipulative", and "disruptive" (*95 percent of most downloaded apps for young kids target them with ads, study finds*, 2018). These ads seem to only advertise other games and educational apps, or lead to crude videos and other questionable content.

In 2018, YouTube Kids was marketed as a safe space for child friendly videos, cartoons, educational clips, and videos designed to entertain children. However, YouTube's advertisement algorithm was bombarding children with links to other videos that have since been come to be called "Elsagate" (named after Disney's Frozen character, Elsa). These crude videos are created using bots, and use keywords to rack up views. They have enough animation to capture the

imagination of the child, while depicting familiar Disney characters in situations "featuring injections and injuries or urination and defecation, some are real adults acting as Elsa/Spiderman/Joker with fetishy sexual undertones, others are crude animations featuring characters buried alive, and the use of machine guns" amongst other disturbing scenarios such as a woman's bikini clad body with Hitler's disembodied head on it, dancing with a skeleton (Hogan & Smith, 2018).

In 2020, YouTube was forced to change their business model due to a landmark settlement they made with the U.S. Federal Trade Commission (FTC). YouTube was fined $170 million for violating the Children's Online Privacy Protection Act (COPPA). COPPA prohibits websites from gathering personal information on anyone under 13 without their parental consent. Although YouTube took the right step in eliminating targeted ads and using machine learning to determine what goes into YouTube Kids, the problem still remains that not all material uploaded is kid material and many YouTubers are having their material mislabeled resulting in less revenue for them, and possibly inappropriate material for children (Dudok de Wit, 2019).

YouTube is only one app amongst millions. Compromised apps may not only try to corrupt young minds, they may also contain malware. In 2020, malware called Tekya surfaced (Hodge, 2020). It is able to imitate the actions of a user and will automatically click on banners and ads, which may be attempts to exploit vulnerabilities such as Cross Site Request Forgery that hijacks a user's session with another legitimate website or app (Wernick et al., 2020). This could cause a user to modify their accounts with other apps or services, or even transfer monies to unknown bank accounts without their knowledge.

Another threat is "AdultSwine" which in 2018 was found embedded in 60 apps designed for kids. However, it was also embedded in thousands of other apps that somehow made it past Google's Android Market verification processes. AdultSwine works by displaying pornographic internet ads, then misleads users into installing fake security apps (to deal with the ads), then

steals the user's data, and registers the users for premium services (real or fake) that add up to actual money in the criminal's pocket (Waqas, 2018), while in the meantime, kids have been exposed to inappropriate material. CheckPoint research refers to these tactics as "Scareware" (Root & Melnykov, 2018). Sadly though there are worse threats lurking for minors that have unrestricted access to the world wide web, or a smart phone with internet.

Fox News reported in 2018, nine popular apps predators were using to target children (Gonzalez, 2018). To avoid becoming overly popular, predatorial apps use obscure app names and the list is extensive (Habas, 2022). Some of these are giants in the industry such as Facebook, Instagram, and Google. Despite the fact that these corporate entities continue to work with law enforcement to stop and capture these predators, the threat persists. The most dangerous apps come from designers who have figured out how to market their product to the general public and burden the users with the risks. This means that minors who lie about their age can gain access to these apps. Snapchat, one of the most popular apps, promises that chats and photos will disappear after a set amount of time, but fail to be transparent about sharing the user's location. Kik allows anonymous contact that bypasses most text messaging controls. Whisper is an anonymous social network that encourages sharing secrets with strangers and also shares the user's location. Calculator% [sic] is an app that is used to hide videos, files, photos and browser history while purposely appearing as a calculator app to parents curious enough to see what apps a child has on their phone (Knight, 2019). These are just to name a few (see Table 1 for list of more apps).

There are also stalker type apps such as TheTruthSpy that not only are designed by malicious actors, but by an entire enterprise seeking to exploit children, in this case a Vietnam based company named 1Byte (Malwarebytes Labs, 2022). TheTruthSpy is marketed as a tool for investigating a loved one, or as a form of parental control. It also states that with this app a user may not require the services of a private investigator. Not only does the app share virtually everything the phone's owner is texting, messaging, their location and social media interactions,

it can be remotely activated to listen in on the owner anywhere at any time without their knowledge (Johnson, 2022). If the invasion of privacy was not enough of a concern, the software itself is vulnerable and open to exploitation. Specifically, the vulnerability being exploited is called an insecure direct object reference, also known as IDOR. It is a bug that exposes data on servers due to poorly written code, or lack of security controls. This would be much like requiring a key to get into a house, but finding that the key also opens all the houses on the block (Whittaker, 2022).

TechCrunch discovered this vulnerability as well as explained 1Byte's operation. The spyware was harvesting information from over 400,000 phones, to include nine other additional apps with identical code, thus having the same vulnerability. These spy apps are not the only vulnerable apps on the market. SpyFone came under scrutiny when the Federal Trade Commission banned it and its CEO Scott Zuckerman from the "surveillance business over allegations that the stalkerware app company secretly harvested and shared data on people's physical movements, phone use, and online activities through a hidden device hack" (Connor, 2021). There were 2,220 people whose information was stolen by hackers in 2018 when they managed to access the company's server because the data was not kept secure (encrypted). To make matters worse, the data stolen was not the consumer's data but data that belonged to the victims being spied upon. Now imagine this software being used on children. There are some measures in place to prevent vulnerable apps from being marketed, but many ask if it is enough.

To help mitigate these threats, the two primary app stores, Apple's iOS store, and Google's Android Market (aka Play Store) have taken steps to prevent the exploitation of users and children. For example, in 2017, Google reported it had removed 700,000 apps in that one year due to malware. This had been a 70% increase over the previous year. This also illustrates the constant battle between these companies and cyber-criminals (Henry, 2018). Both companies have established processes in which apps that have been submitted are reviewed and categorized before granted approval to be in their app stores.

Both companies have published policy and procedures for submitting apps for review. Apple's Guidelines provide clear expectations for apps, especially for children. For example, section 1.3 explicitly states the app cannot include links leading to sites outside the app, cannot present purchasing opportunities as part of gameplay, and all purchase options need to be behind a parental gate (requiring parental intervention to approve and make purchases). It also must comply with privacy laws for children pertaining to what data can be collected, all in accordance with Children's Online Privacy Protection Act (COPPA) (Apple Inc, 2022). Apple also ensures that each and every app and update in their store is approved by an actual Apple employee. An entire division, "App Review", consisting of 300 reviewers, is dedicated to preventing "scammy" apps from being published to their users. As great as this may sound, each reviewer has a daily quota of 50-100 apps they must review. Reviewers are sometimes expected to work 12 hour days, and because every decision can be appealed by Apple's Review Board, every reviewer can face backlash if their decision is overturned (Leswing, 2019). Time is not a consideration built into the review process to truly test the apps for security vulnerabilities, bugs, malicious intent, or review the full experience of the apps content. Although reviewers will catch buggy apps, or violations related to privacy laws, and even well-known scams, such as the Chinese PK10 efforts to commit fraud, the inherent risks in using the apps ultimately fall to the consumer, or the parents.

Google's process is not as articulated as Apple's. Much of Google's documentation is focused on how to interact with the App submission site. This includes "create your app" and "prepare documentation in this format" and "setup your store listing" (Google Inc., n.d.). According to Orangesoft, their step-by-step guide to publishing Android apps includes a step that states, "Study Google Developer Policies" which encourages developers to be familiar with the definition of restricted content, promoting an app's listing, copyright, rules for use of ads, and privacy regulations. The app must be in in APK file format (Android Package) (Kharychkova, 2022).

Interesting note, if the app is not approved to be listed in Google's Play Store, the developers can still release their software to the public, and users can download the APK file to their devices and install the app anyway. Security firm Check Point explains, "although Google actively scans the Play Store for malicious code, policing its vast, ever-evolving catalog of apps is a challenge. The company is 'struggling to keep certain malware outside the App store' because some nasty code can only be detected by dynamically analyzing the context of an app's actions, which is hard to do" (D'Onfro, 2018).

The National Institute of Standards and Technology (NIST) states in their publication, "*Vetting the Security of Mobile Apps,*" that organizations should have a software assurance process that promotes a level of confidence that the software being installed is free from vulnerabilities (both intentional and unintentional), and that the app performs as expected. The Open Web Application Security Project (OWASP) maintains s variety of resources for mobile app testing and security. They also provide a model for app security called the Mobile Application Security Verification Standard (MASVS). All organizations should consider these guides as baselines for their software development processes (Ogata et al., 2019).

It is no surprise that developer's want to make a profit and not spend more time than needed to create a game or add a feature to their app, they should be concerned with their customer's data and device that their software will reside on. Developers also must be familiar with COPPA and the guidelines they prescribe. Amongst these is a list of personal information that cannot be collected on anyone younger than 13: full name; address, email or other identifier; phone numbers; social security numbers; photos or recordings of the child; or geolocation (Designing apps for children: Guide to COPPA and mobile apps, 2013). However, developers can simply list their app for an older audience knowing that kids who want it can lie about their age or find ways around parental controls to get access to the app.

NIST also lists the vulnerabilities common to Apple iOS, and Google Android. Analysis shows that a majority are the same for both, yet some differ. For example, Android has issues

with incorrect permissions being granted in the code, giving too much to the app either through design, or grandfathered. Due to Android's design, if an app wants access to a user's contacts, it must be asked for and granted. Apple iOS also faces issues with incorrect permissions, but the permissions are handled differently so that any installed app automatically inherits permission to sensitive data without explicit permissions granted by the user. For a full chart of these vulnerabilities, see Table 2.

Most smartphone vulnerabilities have been on OWASP's top ten since they started publishing the list, specifically, "Security Misconfiguration", while NIST lists a whopping 43 app vulnerabilities associated with mobile phones. OWASP explains that Security Misconfiguration consists of a plethora of vulnerabilities such as: unnecessary features being enabled or installed, or accounts and privileges granted when not needed; default accounts and passwords unchanged or enabled; cloud services not using appropriate security configurations in the communication protocols; security features not enabled or updated; security settings not set with secure values; or the software itself is simply out of date (*A05 security misconfiguration - OWASP top 10 of 2021*, n.d.).

NIST's 43 vulnerabilities consist of two major categories: "Application Vulnerabilities" and "Malicious or privacy-invasive applications" (*Applications · mobile threat catalogue*, 2022). "WebView App Vulnerable to Browser-Based Attacks" is an App vulnerability that essentially takes advantage of the app when it uses WebView. WebView is when an app opens an internet browsing session within the app and although it may look innocent, can be performing actions in the background, i.e. sending commands to transfer funds from your bank to another account using the tokens or cookies you already have in use from another app or web page. This is called "Cross-Site Request Forgery" (CSRF). It also allows for cross-site scripting or injection of other malicious dynamic content (often through JavaScript) (*APP-8 · mobile threat catalogue*, 2022).

Another vulnerability listed as "Masquerade as Legitimate Application" is better known as a "Trojan". The term comes from Greek mythology when a giant horse was presented as a gift

to Troy as a token of peace, but secretly containing a small force of Greek soldiers. When the horse was accepted, the Greek soldiers successfully infiltrated the city. In cyberspace, the Trojan is software posing as a legitimate app that installs other malicious code or software in the background to gain access to data, the phone itself, or other malware, spyware or ransomware (*APP-14 · mobile threat catalogue*, n.d.).

The common consumer is typically not aware or concerned with these security vulnerabilities when they download and install apps to their devices. Children are even less concerned. However, they are the prime targets or victims of these flaws. The number of permissions found in apps during a study by the FTC can be seen in Table 3.

Keep in mind that Android requires permissions for each of the controls listed, whereas Apple's app review process assumes all apps will require all permissions, therefore when a user downloads an app from the Apple store, that app has full permission to all controls listed in Table 3.

With apps requiring this much access, it is very difficult to ascertain what data is being collected. Furthermore, it is even more difficult to determine how that data is protected once collected, or where, or by whom. Now, user's data, child or adult, is vulnerable due to flaws in app code, and undetermined vulnerabilities in the server where the data resides. There is no guarantee provided to any user on what happens when they use the apps. There is no law that states developers must design security into their software. There is no easy way to see in the app stores if an app is safe for themselves or their children. Apple and Google may exercise due diligence and run tests and check for security vulnerabilities in their own apps, but they are assuming third party app developers are doing the same. This would seem logical and ethical, but as of today, there is no formal code of ethics for app developers, which means there is nothing that prevents them from being misleading or shady with their product. There are some legal requirements an app must meet, but a malicious developer can easily fool the app review boards. Some legalities that the app stores look for are: making sure the app developer agrees

with the store's guidelines; that there is a space reserved somewhere in the app for Terms of Use and Privacy Policy, and possibly and End-user License Agreement (Singh, 2022).

Considering that the Cybersecurity and Infrastructure Security Agency (CISA) reports that kids aged 8-18 spend approximately 7 and a half hours a day online, it seems the focus is misdirected since the guidelines are all about making sure checkboxes are checked rather than protecting children from vulnerabilities that can be exploited to steal their identity, steal their information, or worse, lure them into situations that can become life threatening (Homeland Security, n.d.). If the developers and app stores fail to ensure security and safety, it ultimately falls onto the consumers and parents to do so. Fortunately, there is help.

There are many sources today to assist parents and children in protecting themselves from malicious actors who wish to exploit cyber security vulnerabilities and ultimately those who use apps and the internet. The Internet Crimes Against Children (ICAC) Task Force Program is a suborganization of the Office of Juvenile Justice and Delinquency Prevention (OJJDP), a part of the Department of Justice. They are a "national network of 61 coordinated task forces, representing over 5,400 federal, state, and local law enforcement, dedicated to investigating, prosecuting and developing effective responses to internet crimes against children". The ICAC website goes on to explain that "the program was developed in response to the increasing number of children and teenagers using the Internet, the proliferation of child sexual abuse images available electronically, and heightened online activity by predators seeking unsupervised contact with potential underage victims" (*ICAC - Internet Crimes Against Children Task Force Program*, n.d.). These efforts have seen results. Last year, more than 137,000 investigations and 90,000 forensic examinations were conducted. More than 10,000 individuals were arrested. Effective training has been provided to law enforcement, legal prosecutors, and various other professionals.

In October of 2022, a Bangledeshi National was arrested for operating an international child exploitation enterprise. Zobaidul Amin used an app, Snapchat to "identify and coerce"

children to take photos and videos that were sexually explicit and sadistic. This conduct is also referred to as “Sextortion” (US Attorney’s Office, 2022).

In another case, The National Center for Missing and Exploited Children (NCMEC) shares the story of Amanda Todd, who at 13 became the victim of cyberbullying. Matters got worse when a predator charmed her into become intimate over a webcam by consoling her about the cyberbullying. At 15, she made a YouTube video to share her story in order to help prevent others from following in her steps. Sadly, only a month after her video went viral, she ended her life. The NCMEC runs a CyberTipline specifically for youths like Amanda. In 2021, they received over 29 million reports. According to Lindsey Olson, executive director of the Exploited Children Division, “it only stops when the child either tells an adult or the offender is identified in some sort of law enforcement investigation […] Unfortunately, these cases can have really tragic consequences. Kids can become depressed, and we’ve even seen some cases where children have taken their own lives” (Davis, 2022). Olson goes on to say that prevention is key when saving unsuspecting children from predators.

The Department of Justice would probably agree as they convey the importance of parents being engaged with their children and the cyberspace they inhabit. Parents should know the apps, how to use parental controls and teach their children how to talk to them when something happens or makes them uncomfortable (*Keeping children safe online*, 2021). Parents and teens should be aware of what they are inviting into their home and into their life when they download and install any app. Some apps like Bumble seem teen friendly, but are designed much like Tinder except it requires girls to make first contact. The age limit barrier is easy to bypass by falsifying one’s age. Many apps can seem rather harmless to the parent who is casually sifting through their child’s phone. However, many apps invite a level of anonymity that result in doing things online that would not normally be done in real life. Parents need to be aware and educated on these apps (Knight, 2019).

Some parents may remember in 1983, DARE (Drug Abuse Resistance Program) was established in Los Angeles, California to help battle the drug problem in the schools (*Program profile: Drug Abuse Resistance Education (DARE),* 2011). The program has seen great success in all 50 states and 6 other countries, and is still active today. There is however, no such widespread program for cyber safety, and where drugs is typically a temptation introduced from friends or family, these cyber threats are literally in the hands of children everywhere posing as legitimate apps. CISA provides cyber education for schools or homes that request it. Their Cyber Security Awareness Volunteer Education (C-SAVE) is available to K-12 students. They also provide literature and offer presentations to schools (*Cybersecurity awareness program parent and educator resources*, n.d.). These resources are not integrated in the schools like DARE. The FBI's Safe Online Surfing (SOS) program targets students in grades 3rd through 8th and educate them on how to browse the web safely. Using lessons and games it addresses cyber bullying, avoiding malware, and how to discern if a site is trustworthy (*Parents, Caregivers, Teachers: Protecting Your Kids*, n.d.).

Another program, CyberPatriot, was founded in 2009 by the Center for Infrastructure Assurance and Security (CIAS), and by 2012 had outgrown the system it had created. Partnering with the United States Air Force Reserves, it was fully operational across the country and various nations by 2014. Using a competition-based system, it began by instructing high school students how to harden operating systems such as Windows, Linux, and later introduced CISCO routers. Their education program has evolved to include Middle Schoolers and Elementary kids. They have even gone as far as starting a Senior Citizen program to teach and assist the older generation in the cyberworld, so people of all ages can protect themselves from malicious actors (*CyberPatriot History*, n.d.).

The education is fully engaging, and extremely practical. Coaches are typically teachers who gather the students and interface with parents, arrange field trips, etc. Mentors are volunteers that are vetted (background checks) and are experts in the area of cybersecurity.

Students learn about ethics, viruses, malware and vulnerabilities, computer code and internet safety. The greatest benefit is learning how to harden an operating system. The competitions comprise of teams that are 2-5 students, that must in a 6-hour time-span, find all vulnerabilities on various operating systems and correct them. These vulnerabilities range from user accounts that have the wrong permissions to root kits; from poorly updated software to keyboard loggers. Part of the competition also includes forensics such as doing checksums or decrypting a hidden message. The experience is immeasurable to the students and their parents. For those who spend three years in the program will typically learn enough to acquire a Security + certification minimal study. One mentor reported "that the cyber skills they have learned enrich every participant, as they'll practice them throughout their lives" (Cole, 2020).

Another company, Bark, has made it their mission to not only protect children from online predators, but to empower parents with the ability to be a part of their children's online lives. Bark produced a video to share what they do that teens and parents alike should all take time to view, and with 18 million views, it is a must see (Bark, 2020). Bark does have a parental app, but their focus is to educate children and parents about online behaviors and threats, as they believe that and educated, united family is the best deterrence (Sweeney, 2022). One parent remarked, "With all the potential dangers out there, even with online gaming — cyberbullying, predators, access to age-inappropriate content (and if we're honest, curiosity is INGRAINED in every child, so don't think yours won't go looking) — it's time we included this responsibility under our parental umbrella" (Gruener, 2022).

There are a variety of third-party parental control apps to choose from, especially for Android users, and some may work for Apple devices though Apple relies heavily on their own Parental Gates. There are many articles on the internet that can inform and educate parents on which parental control app is best for them and their family (12 Best Parental Control Apps For IPhone And Android, 2022).

In conclusion, cyberspace is not a playground for children, and certainly not without its dangers. Cyberspace has pirates, criminals, predators, and thieves lurking in the proverbial shadows. Parents should take care to research the age-appropriate ratings on games, apps, and movies, but parents should verify these ratings and not blindly trust those who reviewed the material. It has been shown, that the reviewers don't catch everything that is a danger to children, for if they did, there would not be hundreds of thousands of apps with malware embedded in it. Parents must remember that malware, spyware, ransomware, viruses, trojans, and pornographic material did not accidentally appear or infect the applications. Those apps were designed that way on purpose.

There is an assumption that there is an ethical code for app developers. Aside from making a profit, there is not. There are very real threats targeting the younger generation and they go unnoticed for the most part, until its too late for many young people who are exploited. Major companies like Apple and Google have put measures in place to offer assurance that apps in their stores are safe, yet do not examine the apps sufficiently to consider all the effects they may have on minors. Laws have been put in place, government organizations have been established, all to combat the abuse children suffer from online attacks, yet the number of victims continues to climb. The lack of a persistent presence of cyber security programs are lacking in the schools. Parents are often left out of the picture when it comes to their children's online experiences, many times assuming the apps that are listed as 'kid safe' are indeed safe for kids, when statistics show they probably are not.

Historically, every family, every person in the wild west owned a gun for their protection. To move about unarmed was an invitation to being robbed, taken advantage of, or killed. Today, the wild west lives on in cyberspace, but too many people are moving about in it unarmed and unable to protect themselves from online bandits, thieves and pirates. Parents and children must be educated and made aware of the threats that aren't just out there somewhere, but literally in the palm of their hand.

Table 1

Dangerous Apps for Children and Teens

App ICON	App Name	Description / danger
	Meetme	dating social media app allowing users to connect with people based on geographic proximity. Users are encouraged to meet each other in person. (Knight,2019)
	Grindr	dating app is geared toward gay, bi and transgender people. Users have options to chat, share photos and meet up based on a smart phone's GPS. (Knight,2019)
	Skout	location-based dating app. Users under 17 are unable to share private photos, though kids can easily create an account with an older age. (Knight,2019)
	Whatsapp	messaging app allowing users to send texts, photos, voicemails, and make calls and video chats. (Knight,2019)
	TikTok	used for creating and sharing short videos. Limited privacy controls, so users are vulnerable to cyber bullying and explicit content. (Knight,2019)
	Badoo	dating and social networking app where users can chat, share photos and videos based on location. Intended for adults only, but teens are known to create profiles. (Knight,2019)
	Bumble	similar to Tinder, but requires women to make the first contact. Kids have been known to create fake accounts and falsify their age. (Knight,2019)
	Snapchat	promises users that photos or videos will disappear. Snapchat also allows other users to see a user's location. (Knight,2019)
	Kik	allows anyone to contact and direct message children, sometimes anonymously. Kids sometimes use Kik to bypass traditional text messaging features. Kik gives users unlimited access to anyone, anywhere, anytime. (Knight,2019)
	LiveMe	live-streaming video app uses geolocation to share videos so users can find a broadcaster's exact location. Predators can lure minors to share photos by paying them 'coins' within the app. (Knight,2019)
	Holla	creators of this app admit it as an "addicting" video chat app. Users can meet anyone anywhere in the world. Users are confronted with racial slurs, explicit content, and more. (Knight,2019)

	Whisper	an anonymous social network promoting the sharing of secrets with strangers. A user's location is shared so people can meet up. (Knight,2019)
	Ask.fm	known for cyberbullying. Encourages users to allow people to anonymously ask them questions. (Knight,2019)
	Calculator#	one of several secret apps used to hide photos, videos, files, and browser history. (Knight,2019) For similar apps see list on Safewise.com (8)
	Hot or Not	users rate other users' profiles, with the focus on physical appearance. Focus is to check out people in local area and chat with strangers with the goal to "hook up." (Knight,2019)
	Facebook	Targeted ads and age-inappropriate content, potential to harbor cyberbullying, low self-image, negatively impact mental health, and hinder ability to establish foundation on reality (Kelly & Duffy, 2021)
	Instagram	potential to negatively impact mental health and body image, especially amongst teenage females (Kelly et al., 2021)
	Discord	started as gaming messenger app, evolved into study and organizational app. In 2019 became saturated with predators (Salizar, 2019)
	YouTube	As of 2019, "YouTube has also announced that it will use machine learning to identify unlabeled kids' content. But it admits that such a system 'is not perfect,' so creators of adult content could find their videos incorrectly defined as 'for kids.'" (Dudok de Wit, 2019) Also subject of Elsagate (Hogan & Smith, 2018)
	Zoomerang	video editor that uses location tracking (Habas, 2022)
	Reddit	forum where users share ideas and post comments. Started as bulletins and blogs. Known for posting links and adult content. Many filters still categorize Reddit as a forum (Habas, 2022)
	Photo altering apps or Deepfake apps	apps that alter photos to appear older, younger, beautiful, ugly, gender-swapping, face-swapping, and body-editing apps may require permissions that are not necessary for the app to function (Mekuli, 2022). Be mindful of what permissions are granted (Habas, 2022)
	Social Media apps	other social media apps to be aware of that may have unknown psychological effects, or invite cyberbullying, or other predatorial behaviors: Tumblr, Twitter, QZone, Tout, Spreely, Triller, MeWe, Gab, Rumble, social, IRL, YikYak, Hoop, GETTR, VSCO, WeChat, Wishbone, and Marco Polo (Habas, 2022)

	Live Streaming apps	videos are live and unmonitored, easy for people to say or show whatever they want. Kids can use livestreams to access content blocked elsewhere. Apps include: Houseparty, Big Live, BIGO Live, Uplive, Clover, REALITY, Quibi, Twitch, Tango, Yubo, Livestream, Nonolive, YouNow, Spoon, 17Live, SuperLive, MICO, Imo live, OK Live, Hakuna, Likee, Coco, ly, Camsurf, Omega, Hola (Habas, 2022)
	Messenger Apps	unmonitored, messenger apps could invite strangers to chat with children. Some apps include: Viber, Telegram, Caffeine, Clubhouse, IMVU, Friends, Fam, Threema, Wink, Itsme, BOSS Revolution, Chatjoy, Imo, Nowchat, Signal, ICQ, Hangouts, Addchat, Wizz, BOTIM, BiP, Anonymous Chat Room, Cheers, Squad, Byte, Omegle, Telonym (Habas, 2022)
	Multiplayer Games with built in chats	when not configured properly these chats invite strangers to chat with children. It has been known for predators to falsely portray themselves as a child. Some include, but not limited to: Zepeto, Among Us, PUBG, Suspects: Mystery Mansion, LifeAfter, The Wolf, Call of Duty, Super Mecha Champions, Tom & Jerry: The Chase, Drug Grand Mafia, Modern Combat, Spaceteam, Hago, Rules of Survival, Slam Dunk (Habas, 2022)
	Dating Apps	of those already mentioned, dating apps encourage "hooking up" with strangers and may contain adult oriented content. For full list see list on Safewise.com (Habas, 2022)
	Explicit apps	be aware of apps that make it past the app stores review boards that will contain prolific sexual content. For full list see list on Safewise.com (Habas, 2022)
	Interactive Story apps	apps designed to look like a 'choose your own adventure'. They may look safe until downloaded, but reveal they contain adult content. Some that may seem kid safe are: "Stories: Your Choice", Hotel Hideaway, The Arcana, Producer. For full list see list on Safewise.com (Habas, 2022)

Note. Listed apps are derived from multiple sources cited within the table.

Table 2

NIST's Mobile Threat Catalogue

Type of Vulnerability	APP ID	Threat Name
Application Vulnerabilities	APP-0	Eavesdropping on Unencrypted App Traffic
	APP-1	Man-in-the-middle Attack on Server Authentication
	APP-2	Sensitive Information Exposure
	APP-3	Sensitive Information in System Logs
	APP-4	Need to Use a Known Vulnerable App or Device
	APP-5	Malicious Code Downloaded via Malicious URL
	APP-6	Vulnerable Third-Party Library
	APP-7	Data or Functionality Exposed to Untrusted Apps
	APP-8	WebView App Vulnerable to Browser-Based Attacks
	APP-9	Compromised Backend Server
	APP-10	Poorly Implemented Cryptography
	APP-11	Untrusted Input to Sensitive Operations
Malicious or privacy-invasive	APP-12	Malicious Device Information Gathering
	APP-13	Sensitive Information Discovery via OS APIs
	APP-14	Masquerade as Legitimate Application
	APP-15	Distribution of malicious apps by a 3rd party store
	APP-16	Premium SMS Fraud
	APP-17	Intercepting SMS Messages
	APP-18	Premium Service Fraud
	APP-19	Audio or Video Surveillance
	APP-20	Loading Malicious Code at Runtime
	APP-21	App Vetting Misses Malicious App
	APP-22	Avoiding Uninstallation via Permissions Abuse
	APP-23	Ransoming Assets via Device Management Abuse
	APP-24	Covertly Track Device Location
	APP-25	Abusing Existing Root Access
	APP-26	Privilege Escalation via OS Vulnerability
	APP-27	Persistence via Writing to System Partition
	APP-28	Encrypting and Ransoming Files
	APP-29	Command-and-control Traffic Evades Analysis
	APP-30	Exfiltration Evades Analysis
	APP-31	Masquerading as a Legitimate Application
	APP-32	Exploiting Access to Enterprise Resources
	APP-33	Bypassing OS Private API Controls
	APP-34	App Provides Remote Control Over Device
	APP-35	Retrieving Sensitive Information from Clipboard
	APP-36	Pre-Installed Apps Invading Privacy
	APP-37	Unknowingly Perform Hidden Actions in Other Apps
	APP-38	Abusing Device Resources for Computations
	APP-39	Using Device for DDoS
	APP-40	Capturing Raw Screen Buffer
	APP-41	Recording Audio by Placing or Answering Phone Calls
	APP-42	Malware Uninstalls Itself

Note. Adapted from NIST's Mobile Threat Catalogue (Applications · mobile threat catalogue, 2022).

Table 3

Permissions found in apps in a study by the FTC

Permission	% of Apps	% of Free Apps	% of Paid Apps
Network communication: full internet access	60.99%	78.81%	28.13%
Phone calls: read phone state and identity	20.88%	29.66%	4.69%
Modify/delete SD Card	15.93%	16.95%	14.06%
Fine GPS location	6.04%	7.63%	3.13%
Coarse GPS location	5.49%	7.63%	1.56%
Both fine and coarse GPS location	3.30%	4.24%	1.56%
Hardware controls	3.85%	4.24%	3.13%
Services that cost money	2.20%	3.39%	0%
Modify global system settings	2.75%	3.39%	1.56%
Record audio	1.65%	2.54%	0%
Access personal information / read sensitive log data	0.55%	0.85%	0%
No special permissions	24.18%	13.56%	43.75%

Note. Adapted from "Mobile Apps for Kids: Current Privacy Disclosures are Dis-APP-ointing" (FTC Staff, 2012).

References

12 Best Parental Control Apps For IPhone And Android. (2022). Softwaretestinghelp.com. https://www.softwaretestinghelp.com/parental-control-apps/

95 percent of most downloaded apps for young kids target them with ads, study finds. (2018). CBS News. www.cbsnews.com/news/ads-targeting-children-game-educational-apps/

A05 security misconfiguration - OWASP top 10 of 2021. (n.d.). Owasp.org. Retrieved October 3, 2022, from https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

APP-8 · mobile threat catalogue. (2022). Nist.gov. https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-8.html

APP-14 · mobile threat catalogue. (n.d.). Nist.gov. Retrieved October 5, 2022, from https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-14.html

Apple Inc. (2022). *App Store Review Guidelines*. Apple.com. https://developer.apple.com/app-store/review/guidelines

Applications · mobile threat catalogue. (2022). Nist.gov. https://pages.nist.gov/mobile-threat-catalogue/application.html

Bark. (2020). *Social media dangers exposed by mom posing as 11-year-old*. Youtube. https://www.youtube.com/watch?v=dbg4hNHsc_8

Cole, D. (2020). *Leman Academy CyberPatriot teams top state competition*. Herald/Review Media. https://www.myheraldreview.com/news/classroom/leman-academy-cyberpatriot-teams-top-state-competition/article_d1e1994e-42b8-11ea-b8ee-536b798649dc.html

Connor, J. (2021). *FTC bans SpyFone and CEO from surveillance business and orders company to delete all secretly stolen data*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data

CyberPatriot History. (n.d.). CyberPatriot. Retrieved October 20, 2022, from https://www.uscyberpatriot.org/competition/history

Cybersecurity awareness program parent and educator resources. (n.d.). Cisa.gov. Retrieved October 6, 2022, from https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-parent-and-educator-resources

Davis, P. (2022). *Sextortion: The hidden pandemic*. National Center for Missing & Exploited Children. https://www.missingkids.org/blog/2022/sextortion-the-hidden-pandemic

Designing apps for children: Guide to COPPA and mobile apps. (2013). Iubenda.com; iubenda s.r.l. https://www.iubenda.com/blog/guide-coppa-mobile-apps/

D'Onfro, J. (2018). *Google had to delete 60 apps, many aimed at kids, after they showed users pornographic content*. CNBC. https://www.cnbc.com/2018/01/12/google-deletes-malware-on-apps-for-kids.html

Dudok de Wit, A. (2019). *A new YouTube rule is threatening animation content creators. Here's what you need to know about COPPA*. Cartoon Brew; Cartoon Brew, LLC. https://www.cartoonbrew.com/artist-rights/a-new-youtube-rule-is-threatening-animation-content-creators-heres-what-you-need-to-know-about-coppa-182883.html

FTC Staff. (2012). *Mobile Apps for Kids: Current Privacy Disclosures are Dis-APP-ointing*. Ftc.gov. https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf

Gonzalez, L. (2018). *Predators using apps to target children*. KMPH. https://kmph.com/news/local/predators-using-apps-to-target-children

Google Inc. (n.d.). *Create and set up your app*. Google.com. Retrieved October 23, 2022, from https://support.google.com/googleplay/android-developer/answer/9859152?hl=en

Gruener, H. (2022). *A mom's review of the Bark app after testing it out [2022]*. Word From The Bird. https://wordfromthebird.blog/the-blog/bark-parental-control-review-honest/

Habas, C. (2022). *Dangerous apps for kids*. SafeWise. https://www.safewise.com/dangerous-apps-for-kids/

Henry, J. (2018). *Malicious apps: For play or prey?* United States Cybersecurity Magazine. https://www.uscybersecurity.net/malicious-apps/

Hodge, R. (2020). *Malware found lurking in kids' Play Store apps, security firm finds*. CNET. https://www.cnet.com/news/privacy/malware-found-lurking-in-kids-play-store-apps-security-firm-finds/

Hogan, R., & Smith, D. (2018). *Elsagate hellscape: The dark underbelly of YouTube Kids —*. Hunt A Killer. https://members.huntakiller.com/blog-articles/2018/1/24/elsagate-hellscape-the-dark-underbelly-of-youtube-kids

Homeland Security. (n.d.). *National Cybersecurity Awareness Campaign - Kids Presentation*. Cisa.gov. Retrieved September 29, 2022, from cisa.gov/sites/default/files/publications/Kids%20Cybersecurity%20Presentation.pdf

ICAC - Internet Crimes Against Children Task Force Program. (n.d.). Icactaskforce.org. Retrieved October 4, 2022, from https://www.icactaskforce.org/

Johnson, A. (2022). *TheTruthSpy: Your #1 mobile Spy app - Free & invisible*. TheTruthSpy; Allen Johnson. https://thetruthspy.com

Joint Task Force. (2020). *NIST SP 800-53 - Revision 5: Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-53r5

Keeping children safe online. (2021). Justice.gov. https://www.justice.gov/coronavirus/keeping-children-safe-online

Kelly, S. M., & Duffy, C. (2021). Facebook whistleblower testifies company 'is operating in the shadows, hiding its research from public scrutiny.' *CNN*. https://www.cnn.com/2021/10/05/tech/facebook-whistleblower-testify/index.html

Kelly, S. M., Gonzalez, J., & Barrett, S. (2021). *Parents of the social media generation are not OK*. CNN. https://us.cnn.com/2021/12/08/tech/social-media-parents/index.html

Kharychkova, A. (2022). *How to publish an Android app on Google Play Store: A step-by-step guide*. Orangesoft. https://orangesoft.co/blog/how-to-publish-an-android-app-on-google-play-store

Knight, T. (2019). *Sarasota sheriff warns parents about 15 apps that could be used to target children*. FOX 13 Tampa Bay. https://www.fox13news.com/news/sarasota-sheriff-warns-parents-about-15-apps-that-could-be-used-to-target-children

Leswing, K. (2019). *Inside Apple's team that greenlights iPhone apps for the App Store*. CNBC. https://www.cnbc.com/2019/06/21/how-apples-app-review-process-for-the-app-store-works.html

Malwarebytes Labs. (2022). *Photos of kids taken from spyware-ridden phones found exposed on the internet*. Malwarebytes. https://www.malwarebytes.com/blog/news/2022/06/photos-of-kids-taken-from-spyware-ridden-phones-found-exposed-on-the-internet

Maxwell, T. (2020). *Malware in Android children's games and utility apps milked 1 million devices for ad clicks*. Input. https://www.inputmag.com/tech/malware-in-kids-games-on-android-milked-1-million-devices-for-ad-clicks

Medaris, M., & Girouard, C. (2002). *Protecting children in cyberspace: The ICAC Task Force program*. Ncjrs.gov. https://www.ncjrs.gov/html/ojjdp/jjbul2001_12_5/contents.html

Mekuli, A. (2022). *How Invasive are Face-Transforming Apps?* Vpnoverview.com. https://vpnoverview.com/privacy/apps/face-transforming-apps/

Ogata, M., Franklin, J., Voas, J., Sritapan, V., & Quirolgico, S. (2019). *NIST SP 800-163 - Revision 1: Vetting the security of mobile applications*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-163r1

Parents, Caregivers, Teachers: Protecting Your Kids. (n.d.). Federal Bureau of Investigation. Retrieved October 6, 2022, from https://www.fbi.gov/how-we-can-help-you/parents-and-caregivers-protecting-your-kids

Program profile: Drug Abuse Resistance Education (DARE). (2011). CrimeSolutions, National Institute of Justice. https://crimesolutions.ojp.gov/ratedprograms/99

Root, E., & Melnykov, B. (2018). *Malware displaying porn ads discovered in game apps on Google Play*. Check Point Research. https://research.checkpoint.com/2018/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

Salizar, M. (2019). *Warning about mobile apps used to target children*. FOX 26 Houston. www.fox26houston.com/news/warning-about-mobile-apps-used-to-target-children

Singh, P. (2022). *Top legal issues to consider for mobile app development*. Appinventiv. https://appinventiv.com/blog/top-legal-issues-in-mobile-app-development

Sweeney, J. (2022). *Bark parental control review 2022 — is it worth the cost?* SafetyDetectives. https://www.safetydetectives.com/best-parental-control/bark

The Morris worm. (2018). Federal Bureau of Investigation. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

US Attorney's Office. (2022). *Bangladeshi national arrested in Malaysia for operating an international child exploitation enterprise*. Justice.gov. https://www.justice.gov/usao-ak/pr/bangladeshi-national-arrested-malaysia-operating-international-child-exploitation

Waqas. (2018). 60 Android apps for kids found infected with Pornographic malware. *HackRead | Latest Cyber Crime - InfoSec- Tech - Hacking News*. https://www.hackread.com/android-apps-for-kids-with-pornographic-malware/

Wernick, I., Golubenko, D., & Hazum, A. (2020). *Google Play store played again - Tekya clicker hides in 24 children's games and 32 utility apps*. Check Point Research.

https://research.checkpoint.com/2020/google-play-store-played-again-tekya-clicker-hides-in-24-childrens-games-and-32-utility-apps/

Whittaker, Z. (2022). Behind the stalkerware network spilling the private phone data of hundreds of thousands. *TechCrunch*. https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/