Cyber Safety for Teens

Essential Tips for Staying Protected Online

By Eric N. Peterson

Cyber Safety for Teens

Essential Tips for Staying Protected Online

By Eric N. Peterson

For Dahri

Copyright

To request permission for use:
Email eric@cybertipsguide.com or eric@nextlevelsecure.com or call 801-682-9682.

First Book Edition: October 2023

Published by Eric N. Peterson

Cover and book design and layout by Eric N. Peterson

Contents

Introduction

Teenagers spend a lot of their time online. From social media to games, schoolwork and studying, connecting with friends around the world, etc. Though the internet has a lot to offer, it comes with hidden dangers and risks. Teens' cyber safety isn't just about keeping their devices and data safe; it's also about keeping their thoughts and lives safe. Even though the online world can be a big place to play in, it also has dangers like abuse, online predators, phishing scams, malware, identify theft and more. Teens need to be aware and careful as they move throughout the digital world. This guide is meant to give teens the information and tools they need to stay safe in the interconnected world of the 21st century and make good choices.

Overview – The Importance of Cyber Safety for Teens

There are eight areas of cyber risk and safety for teenagers, let's take a look.

Digital trace and Reputation: Every time a teenager does something online, like post a picture, leave a comment, or even just search, they leave a digital trace. If they do things that are rude or careless online, it could hurt their image and their chances of getting into college or getting a job in the future.

Personal Privacy and Security: Teens are at risk of having their privacy broken because they share more and more personal information online. Identity theft, scams, and even blackmail can all be done with personal information. Having safe internet habits can help you avoid these dangers.

Cyberbullying and Mental Health: Cyberbullying has been linked to depression, anxiety, and even suicidal thoughts, among other mental health problems. It's important for kids' mental health that they know how to behave online and how to deal with and report online harassment.

Online Predators: Teenagers are especially sensitive to online predators who try to get them to talk to them. These people often wear masks, use tricks, and take advantage of young people's natural wonder and trusting nature for bad reasons.

Financial safety: With the rise of online shopping and in-app purchases, more and more financial tools are available online to teens. Without proper direction, they might fall for scams or make bad choices about their money.

Misinformation and radicalization: There is a lot of false information on the internet. Teenagers need to know how to use the Internet so they can tell the difference between true and fake information. This is also important so that they don't get swayed by extreme ideas.

Exposure to Inappropriate Content: Because the internet is so big, kids can accidentally find content that is too explicit, violent, or disturbing for them. Cyber safety steps help make sure that online experiences are age-appropriate.

Dependency and addiction: Teens who have unlimited access to online games, social media, and other digital activities may spend too much time in front of a screen. This can hurt their health, affect how they sleep, and make it harder for them to make friends in real life.

With its mix of possibilities and threats, the digital realm is a lot like the real world in terms of how complicated it is. Teenagers are still figuring out who they are and what they think about the world, so they need to know how to use the Internet safely. Cyber safety makes sure that they get the most out of the benefits of the digital age while staying safe from its possible dangers.

Why Teenagers are Targeted Online

Generation Born Digital: Tech-Savvy but Naive

Teenagers today were born and raised in a time when technology was everywhere. Because of this, they know how to use the internet, apps, and gadgets well. But their technical skills are often at odds with their lack of life experience, so they don't understand the greater effects and risks of what they do online. Their trust in being able to get around in the digital world can make them miss some of its dangers.

Teens' Data: Driving Consumer Behavior and Marketing

Teenagers are an important group for marketers and companies to target. Companies can make their goods, advertising strategies, and future plans more relevant to teens if they know what they like, what they do, and how they act. This makes kid data a valuable target for both good businesses and bad people who want to use this information for their own gain.

Trends and Challenges: Peer Influence and the Power of Going Viral

Teenagers have a strong need to be accepted by their peers and feel like they fit. This makes people more likely to be influenced by their peers online. Trends and challenges that go viral among teens can spread quickly. Teens may join in without fully understanding the risks or effects, just to get online approval or to "fit in."

Teenagers are Easy Targets for Grooming and Predatory Behavior

Online predators know that teens are often vulnerable because they want to be liked, are curious, or want to rebel. Predators may try to get teens to trust them by giving them care, understanding, or gifts. Their end goals can be as simple as getting personal information or as bad as hurting people. Teenagers are especially at risk in the vast, faceless online world.

Teenagers may know how the digital world works, but their natural development and the high value of their data make them good targets in the online world.

Real-life Stories & Examples

The Chatroom Predator:

> Sarah, a 14-year-old, started chatting with Jake, who claimed to be a 16-year-old from a nearby city, in an online chatroom. Over time, they built a seemingly deep connection. Jake convinced Sarah to share personal details and photographs. Later, it was revealed that "Jake" was, in fact, a 40-year-old man who had been grooming multiple teenagers online. Fortunately, Sarah's parents discovered the conversations and involved law enforcement before any physical meeting took place.

Sextortion: The Dangers of Putting Your Trust in a Stranger Online

> Jamie, a 16-year-old, used social media often to connect with friends and sometimes meet new people who liked the same things she did. Jamie got a friend request from Alex, who seemed to be about the same age as Jamie. They became friends because they liked the same kinds of things and because they liked the same kinds of music.

> The Trap: Alex talked to Jamie for a few weeks and got her to share intimate pictures with him. Jamie unwillingly agreed because she trusted Alex and thought their conversations were private. Alex's tone changed soon after, though. The once-friendly chat buddy started saying that he would show Jamie's pictures to his friends, family, and the rest of the school if Jamie didn't pay a lot of money or give him more embarrassing content.
>
> Outcome: Jamie was scared and didn't know what to do, so she told a close friend. Her friend told her to tell an adult. With the help of their parents, the incident was reported to local police and the social media site. Even though the emotional toll was high, more abuse was stopped because people reported it quickly and helped.

The Fortnite Scam:

> Timothy, a 15-year-old avid gamer, came across an online ad offering free in-game currency for Fortnite if he entered his game login details. Eager to gain an advantage in the game, Timothy provided the information. Soon after, he discovered unauthorized purchases on his account and his personal details were sold on the dark web.

Cyberbullying on Social Media:

> Mia, 13, was excited to share a video of herself dancing on a social media platform. However, a group of schoolmates downloaded the video, edited it with mocking comments, and reshared it. The video went viral in her school, leading Mia to face intense cyberbullying and humiliation. This incident affected her mental health significantly and raised awareness in her community about the adverse impacts of cyberbullying.

Phishing Via Job Offers:

> Alex, 17, was looking for a part-time job to save for college. He received an email, seemingly from a well-known retail chain, offering him a position. The email requested his personal details for background verification. Without verifying the legitimacy of the email, Alex shared his information. It turned out to be a phishing scam, and his data was compromised.

The Viral Challenge Trap:

> The "Blue Whale Challenge" is a sinister example of how dangerous online trends can be for impressionable teens. This so-called "game" allegedly consisted of a series of tasks assigned to players by administrators over 50 days, with the final challenge urging the player to commit suicide. Several teenagers across the globe reportedly fell victim to this malicious online trend.

These real-life instances underscore the importance of cyber safety education for teenagers. Awareness and understanding of such threats can empower them to navigate the digital world securely and responsibly.

Cyber Threats from Gaming Platforms

Malware and Phishing in Mods and Downloadable Content:

Many teenagers are interested in the idea that downloadable content (DLC) and modifications (mods) can make their game experience better. But not all of the places where you can get these downloads are reliable. Malicious people often use popular DLCs or mods to hide malware or hacking tools. Once downloaded, these can damage the user's system, steal personal information, or even lock the machine and ask for a ransom.

The Risks of Chat and Voice Communication in Games:

Chat and voice contact tools in games let players work together and interact in real time. But they can also expose kids to bad language, cyberbullying, or contact from strangers that they didn't ask for. Also, without the physical clues that come with face-to-face communication, it's easier for bad people to hide who they are and what they want.

Scams involving In-game Money and Purchases:

Microtransactions, in which players can buy in-game items or currency, have become more popular in the gaming business. Scammers often take advantage of this trend by using third-party platforms to offer "deals" or "discounts" on these purchases. Teenagers who don't know better could give out their payment information and end up being victims of fraud or illegal transactions.

Online Predators and Grooming on Gaming Sites:

Gaming sites are more than just places to play games; they are also places to meet other people. More and more, predators are using these sites to find possible victims. They could give them gifts in-game, get to know them, and then try to move the talk to a more private channel. Teens need to be careful about who they trust when they play games because they can talk to other people and they can be anonymous.

Even though gaming platforms offer a fun mix of entertainment, competition, and social contact, they also have some downsides. As the digital world changes, so do the possible dangers that could be hiding there. Teenagers can sometimes be too caught up in the game to realize how dangerous it is. Some of the dangers include malware that looks like mods, predators hiding behind nice avatars, and financial scams that look like in-game deals. As these platforms become more important to our lives, it's important that we give our younger generations the information and tools they need to use them safely. Virtual battles in games can only stay fun places to play if people are aware of them, stay alert, and learn about them.

Social Media Risks for Teens

Too Much Personal Information Sharing: Privacy Concerns

Social media sites make it easy for people to talk about themselves, which can lead teens to share more personal information than is wise. This oversharing can be about places, habits, family information, and more. Because of this, they may become objects of stalking, identity theft, or other bad things. Also, once this information is online, it can be hard to get rid of, which could lead to long-term privacy problems.

Cyberbullying and Harassment Online:

Bullying has moved from the real world into cyberspace as a result of the Internet. Harassment on social media can take many forms, like making mean comments or spreading false stories. Bullies can feel more confident on the internet because they don't have to give their names. This leaves teens open to persistent and broad attacks that can have serious emotional effects.

Scams, Phishing, and Faked or Spoofed Accounts:

Teens often take what people say to them on social media at face value. Scammers can use fake accounts or scams to take advantage of this trust. Teens who don't know better could click on harmful links, give out private information, or even be tricked into making fake money transfers.

Sextortion:

These are horrible situations and some end tragically. Follow these recommendations to avoid these scenarios.

1) Be careful about sharing personal or private information, even with people you "know" online.
2) Keep in mind that once something is shared online, it's almost hard to stop it from getting out there.
3) In cases of blackmail or bribery, it's important to get help right away from trusted adults or the police. Trying to handle a problem on your own can often make it worse.
4) It's important to remember that sextortion cases are complicated and can have a big effect on the victims' minds. Cyber knowledge and safety efforts must put a lot of focus on open communication and provide resources for help.

Exposure to Unsuitable or Dangerous Content:

Social media sites have a lot of different kinds of material, and not all of it is appropriate for younger viewers. Teenagers can stumble upon explicit content, extremist ideas, or graphic pictures. This kind of unwanted contact can have a long-lasting effect on a person's emotions and mind.

Comparisons, Self-esteem, and Addiction: How Social Media Affects Our Minds

Social media can skew reality by making it easy to compare lives based on carefully chosen posts and highlight reels. For kids, who are in a very important stage of figuring out who they are and how much they are worth, this can lead to feelings of not being good enough or low self-esteem. Also, the dopamine-driven feedback loops of likes, shares, and notifications can lead to addiction, which can lead to spending too much time in front of a computer, not getting enough sleep, and having fewer real-life social interactions.

In conclusion, social media platforms give teens a place to express themselves, connect with others, and find out about new things. However, they are also full of risks. Teens need to know about these possible dangers and talk openly about them in order to have a safe and good online experience.

Recommendations for Teens Who Play Games

Using Trustworthy Sources to Download and Buy Games:

Teenagers should only download games and related material from well-known, trustworthy sources to avoid malware, phishing attacks, and other scams. This means using official game stores, the developers' websites, or known third-party platforms. If you stay away from "too good to be true" deals on sites you don't know, you can avoid many possible threats.

Limits on Chat and Voice Communication in Games:

In-game communication can make multiplayer games more fun, but it can also put kids at risk of unwanted contact, bad language, and cyberbullying. Parents or guardians can use parental control settings to limit or watch chat features, making sure that younger players can talk to each other in a safe way.

In-game Purchase Education:

Sometimes, microtransactions can make it hard to tell the difference between fictional and real value. Teens should be taught about the costs of in-game purchases and reminded that virtual things cost money in the real world. Setting limits on how much you can spend or asking your parents for permission before you buy something can also be helpful.

Harden All Passwords for Gaming Accounts

A strong password is the first line of defense against people who shouldn't be able to get in. Teenagers should be told to use unique passwords that include a mix of letters, numbers, and symbols for their game accounts if not a pass phrase. Also, if enabled, use two-factor authentication using an authenticator app versus text. This can add an extra layer of security and is highly recommended.

By following these few tips, teens can enjoy the excitement of online games while minimizing the risks potential risks. When it comes to safety, being proactive keeps the digital playground both fun and safe.

Social Media Safety for Teens

Increase your Privacy Settings:

Adjusting the privacy settings on social media sites is one of the first things you can do to reduce cyber risk. Teens should learn how to make their profiles secret so that only people they know and trust can see what they post. By understanding and implementing this, they can avoid accidentally sharing information with a wider audience. This makes them less vulnerable to threats.

Recognizing Suspicious Accounts or Content and Reporting It:

On social media, not everything is real. Teenagers need to be taught how to spot fake or dangerous accounts. This could include sites that share links that aren't what they seem to be, spread false information, or contact people without being asked. If you can recognize these warning signs and research how to report them, you can help keep the platform and yourself safe.

The Dangers of Sharing Location Data and Personal Information:

Teens can be stalked or get unwanted attention if they check in, share their position, or talk about their daily routines. It's important to teach them about the risks of sharing this kind of knowledge. Even things that seem harmless can be used to build a full picture that can be used to the cyber criminal’s advantage.

Talk About Online Experiences and Interactions:

Communication is a key part of remaining safe online. Teens should feel safe talking to trusted adults about their online interactions, both good and bad. Whether it's about a new online friend, a weird message they got, or peer pressure to join a viral trend, these talks can help guide, reassure, and, if necessary, prevent a potentially bad decision.

In this age of digital connectivity, safe ways to use social media aren't just about keeping data safe; they're also about keeping our young people safe. Teens can use social media with ease and also be cyber safe if they understand the risk, know what they're doing and can talk to their parents and friends about it openly.

General Cyber Safety Tips for Teens

Strong, and Unique Passwords, Multifactor Authentication, and Password Managers:

Passwords are the digital keys to our online lives. Teens should be shown how to make strong passwords that are different for each online account. To make these passwords more secure, they should include letters, numbers, and symbols or use pass phrases. They should use password managers, which store and fill in passwords securely and make it easier to manage all the different passwords without compromising security.

Recognizing Scam Emails and Phishing Messages:

Phishing scams try to get people to give out personal information by sending them fake emails or texts. Teens need to be taught how to spot these kinds of scams, like when they get a message they didn't ask for, a file they didn't expect, an urgent tone, or a message from someone they don't know. They should be told to never open strange email links or download files from unknown sources. This includes links in texts or other social media messaging platforms.

Apply Updates Quickly:

Updates to software don't just add new features; they also often include changes that fix security holes such as for zero-day threats. Teens should be encouraged to keep the operating systems, apps, and software on their devices up to date so they can take advantage of the latest security improvements and avoid being attacked using an outdated (exploited and vulnerable) application.

Using Virus and Malware Protection:

Protection tools like antivirus and antimalware software add an extra layer of defense against harmful dangers. Teens should be told to install reputable antivirus and antimalware software and make sure it gets updated often so it can spot and stop the newest threats. This is especially important for Android devices and all desktops and laptops.

Browsing the Internet Safely: Recognizing and Avoiding Suspicious Websites

The internet is a big place, and not every part of it is safe. Teens should be taught how to spot websites that aren't safe, like ones that don't use HTTPS, have spoofed or incorrect domain names (YoTube vs YouTube, but they're not always that obvious), or are full of pop-ups or strange Ads. Using the security tools and features of your computer can also help you find and block dangerous sites.

In a digital age where the lines between the real world and the virtual world are blurry, online safety is a part of personal safety. By giving teens these basic tips, we give them the tools they need to explore the online world safely, which helps them develop a sense of responsibility and awareness.

Educating and Empowering Teens

Here are some strategies for educating and empowering your teens.

Have Open Conversations: Giving teenagers a safe place to talk about their online experiences

It's very important to create a space where teens feel safe talking about their online and social interactions. Having open lines of communication makes sure they get help and reassurance, whether they've seen something strange, been cyberbullied, or are just interested in something new. Trust and understanding, not punishment, will get teens to talk openly and ask for help when they don't know what to do.

Cyber Safety Resources:

In the digital world, the best protection is knowledge. We give teens the tools they need to deal with online problems by pointing them to reliable sources, like informative websites, insightful books, and full-length classes. These tools can help them learn about the different kinds of online threats, how important personal information is, and how to stay safe.

Online and Offline Realities are Different:

Most of the time, the digital world shows a curated or altered version of truth. Teenagers need to be able to tell the difference between the identities people use online and the ones they use in real life. Knowing that online exchanges can be faked or manipulated will help teens be more careful when using technology and keep a healthy balance between their online and offline lives.

Finally, education and empowerment are the keys to making teens' internet lives safer. By giving them the knowledge, tools, and confidence, they need to make well-informed choices, we can make sure that they not only survive but also thrive in the digital age of interconnectedness.

Conclusion

The digital world is constantly changing, such as the way we talk to each other, how we learn, and how we live. With every new technology comes a new set of problems. This makes it even more important for teens to be safe online. As they move through this ever-changing environment, they need to stay alert and keep learning. It's not just about keeping an eye out for possible threats; it's also about helping people become smart and well-informed online. So, the call to action is clear: Teenagers can't just use the internet world without doing anything to keep themselves safe. By taking charge, learning as much as they can, and following safe online habits, they can easily navigate the vastness of the internet, leveraging its power while staying safe online.

About the Author

Eric Peterson is a cybersecurity expert from SLC, UT, working in CyberOps, directing and managing teams that monitor and respond to cyber threats and that help to keep companies' data and enterprises safe. He has over 25 years of experience in IT and Cybersecurity, an M.S. and B.S. in IT Security and assurance, and over 20 industry-recognized certifications, including CISSP, CISM, CRISC, and CISA. As a published author, he has written multiple eBooks, many on guitar instruction, and many cybersecurity technical blog posts and guides.

For more information, connect with Eric on LinkedIn or visit www.cybertipsguide.com for more eBooks and helpful cyber tips and guides.

CYBER TIPS GUIDE

Making Sense of Cyber Safety