Bitdefender® Global Leader In Cybersecurity

Comprehensive Cybersecurity Guide

FOR KIDS

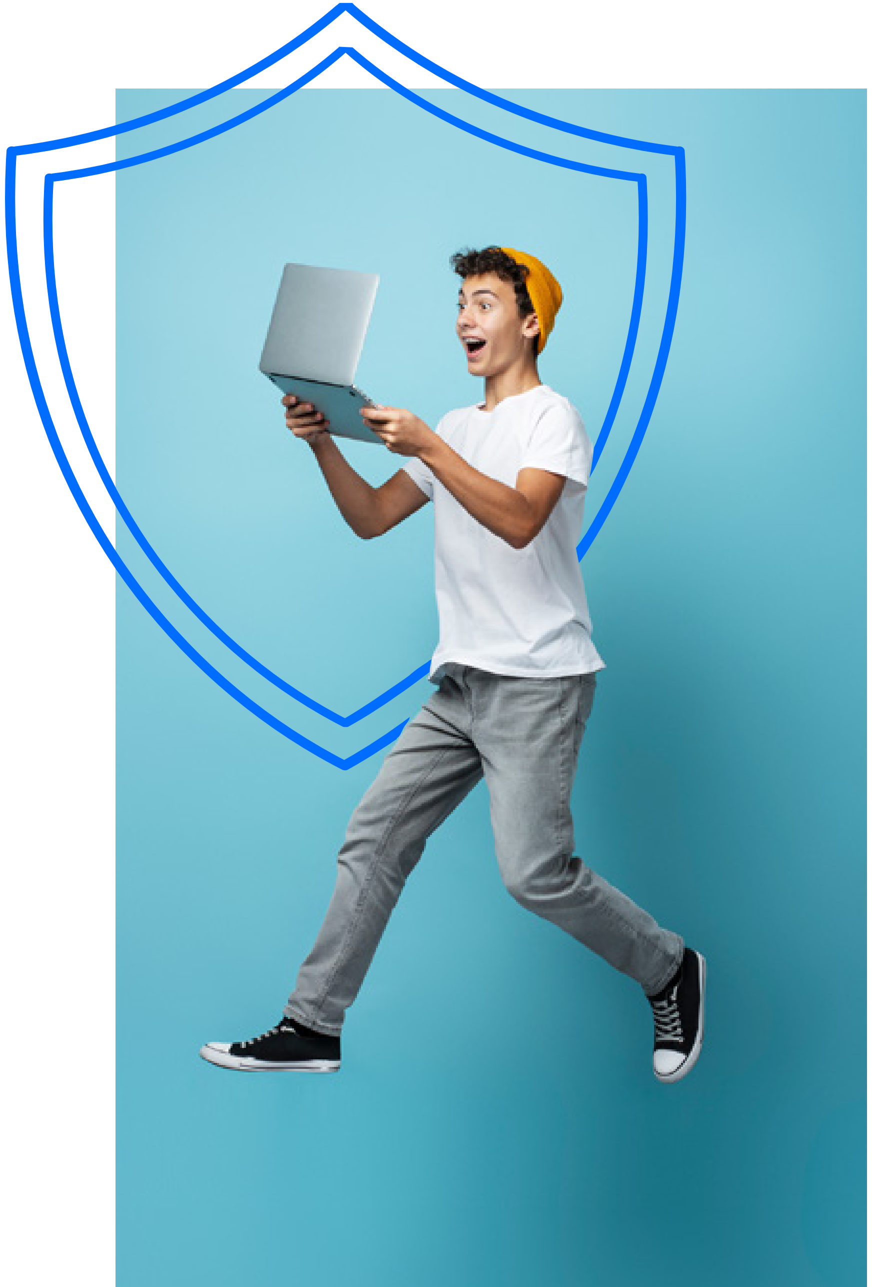
2024

Content:

Introduction

The digital world is vast and exciting, offering endless opportunities for learning, entertainment, and socializing. In the online realm, computers, smartphones, and all connected gadgets collect and gather information, allowing you to chat with friends and family, watch videos, play games, and learn.

However, it's also a place where one must be cautious and smart to stay safe.



Your Digital Footprint and online reputation

Understanding Your Digital Footprint

What do you know about your digital footprint? Can you give an example of something that might be part of it?

What is a Digital Footprint?

A digital footprint is the trail of data you leave behind whenever you use the Internet. Think of it like a trail of clues or like **footprints** you leave behind when walking on a sandy beach.

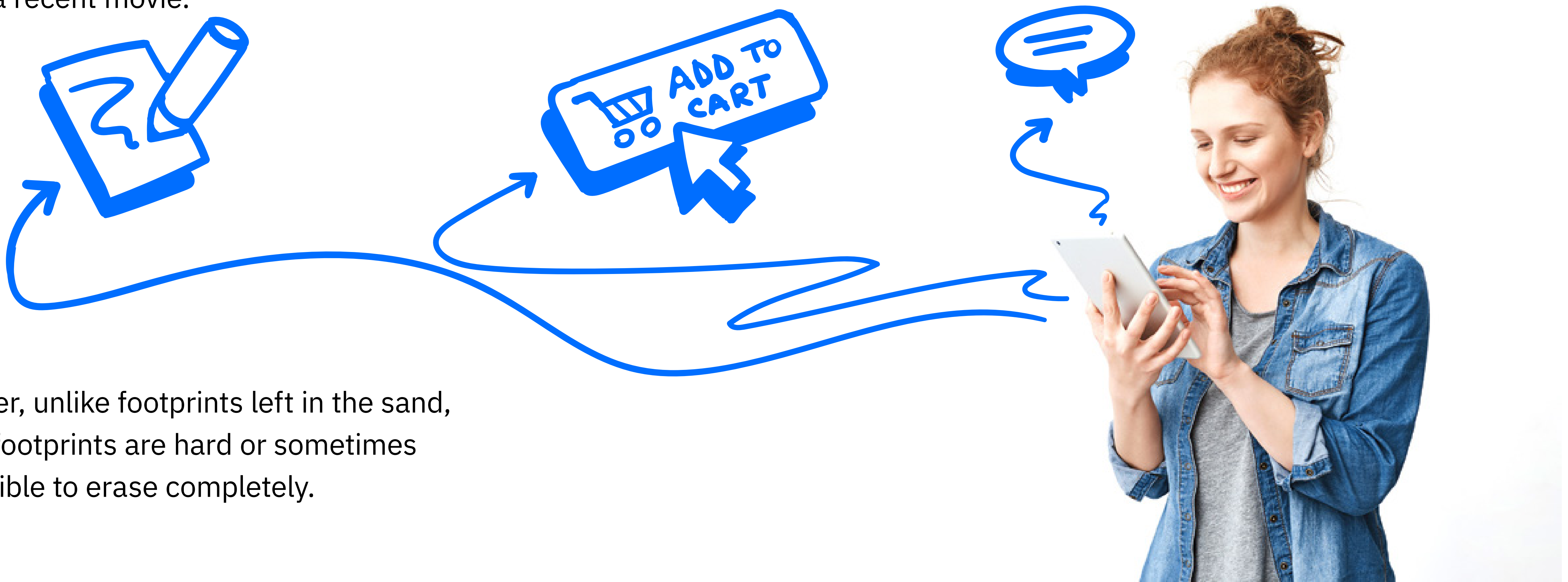
Every time you visit a website, post, send messages or browse, you leave little traces of your activity online. This includes everything from your social media activity (comments and posts), things you search for on Google and videos or photos you upload

Examples of Digital Footprint:

1. Social Media Posts:
Posting a picture of your school event or sharing your thoughts about a recent movie.

2. Online Purchases:
Buying a game from an online store leaves a record of your purchase.

3. Comments on Websites:
Leaving comments on a YouTube video or a blog post.



However, unlike footprints left in the sand, digital footprints are hard or sometimes impossible to erase completely.

Why is Your Digital Footprint Important?

Digital footprints expand and grow alongside you, creating a detailed record of who you are. At the same time, it provides bad individuals, scammers and hackers the means to harm you and your loved ones. Here are some examples of how your digital footprint can impact you in terms of:

Privacy:

Information shared online can be accessed by others, sometimes even by people you don't know.

Reputation:

What you post online can affect how others perceive you now and in the future.

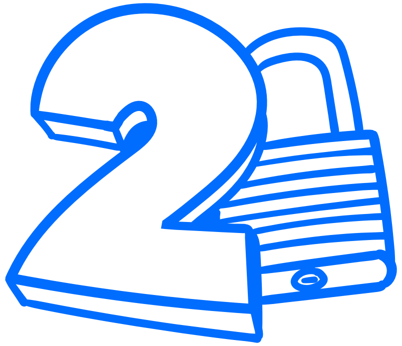
Security:

Personal information can be misused by cybercriminals for scams and identity theft.

Tips to Manage Your Digital Footprint

Think Before You Post:

Ask yourself if you’re comfortable with everyone seeing your post, and never post anything that can harm others or make you look bad.



Privacy Settings:

Use privacy settings on social media to control who can see your information.

Be Cautious with Personal Information:

Never sensitive information like your address, phone number, or school name online.

Your Online Reputation

Have you ever thought about the consequences of bad digital conduct, such as posting a rude comment or inappropriate picture of yourself or a classmate?

What is Online Reputation?

Your online reputation is the perception that others have of you based on your digital footprint. This includes **everything** from social media posts to comments on forums and online interactions.

Colleges and future employers use the internet to search or gather information about candidates, screening social media profiles for positive signs or online misconduct.

Why is Online Reputation Important?

Why do you think colleges and employers might look at your social media profiles? How could what you post online affect your future?

Your online reputation matters more than you think. It can impact:

Future Opportunities:

Colleges, universities, and potential employers often look at online profiles to gauge character and suitability.

Example:
A university might check your social media profiles during the admissions process. Inappropriate posts or comments could negatively impact your chances of getting accepted.

Example:
Employers may look at your online activity to see if you are a good fit for their company culture. Professionalism and positive interactions can improve your prospects.

Relationships:

Friends, family, and peers may judge you based on what they see online.

Example: What you share online can affect your relationships with friends and classmates. Negative or hurtful posts can lead to conflicts or lost friendships.

Safety:

A positive online reputation can help protect you from cyberbullying and other negative online behaviors.

Example: A mean or rude comment you made some time ago or a photo or video can be used to harm you.

How to Maintain a Positive Online Reputation:

Think Long-Term: Consider how your posts might be viewed years from now.

Be Respectful: Treat others with kindness and respect online.

Show Positivity: Share achievements, hobbies, and positive experiences.

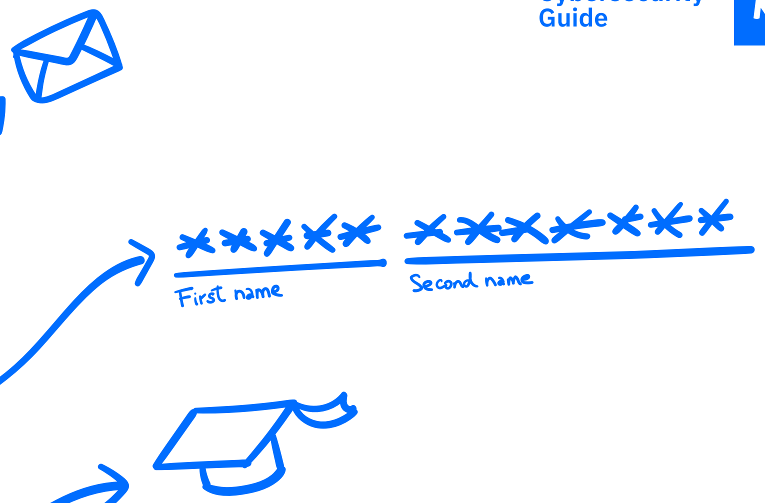
Avoid Controversy: Stay away from engaging in online arguments or posting inflammatory content.

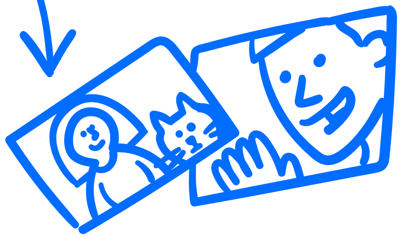
Review: Periodically review your online profiles and remove any content that might be harmful or no longer represents you.

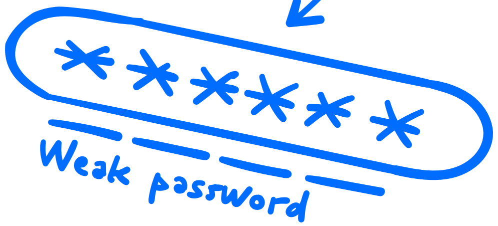
Safeguarding Personal Information

What are some examples of personal information? Why do you think it's important to keep your personal information private when you're online?

Personal information or personal data refers to any details that tell people who you are and how to find you. This can include your full name, home address, phone number, email address, birthday, social security number, school name, personal photos and videos, and even passwords.







Why Safeguard Your Personal Information?

As we said, your personal data creates a clear picture of you. It represents you and can be used to pinpoint your location and cause you harm. Safeguarding it is very important because it helps:

Prevent Identity Theft: Cybercriminals can use your personal information to steal your identity.

Avoid Scams: Scammers often use personal information to trick you into giving them money or more information.

Avoid Extortion: A bully or a bad individual can use personal data you share, including photos and videos, to threaten and intimidate you to gain money or coerce you into making inappropriate decisions.

Protect Your Privacy: Keeping your information private helps maintain your safety and privacy.

Easy Tips to Help Keep Personal Information Safe

Use Strong Passwords: Create strong, unique passwords for each account and change them regularly. Keep your passwords private and don't share them, even with friends.

Be Wary of Unknown Links: Avoid clicking on links or downloading attachments from unknown sources.

Don’t Overshare: Be mindful of what you share online. Never share personal data with strangers you meet online, via social media, or any other apps (gaming, messaging, etc.)

Password-Protect Devices: Your smartphone, laptop, or other smart device should always be password-protected in case of loss or theft. Never leave devices unattended.

Social Media Platforms: Risks and Appropriate Age

How do you decide what to share and what not to share on social media? What are some of your go-to social media platforms and what do you use them for?

Social media can be a fun way to connect with friends and share their interests, but it's essential to use it safely and responsibly.

Most social media platforms (Facebook, Instagram, Snapchat, TikTok, and X) have age limits, usually requiring users to be at least 13. **Did you know?**

Risks of Using Social Media:

Privacy Risks:

Personal information can be exposed if privacy settings are not appropriately managed. Oversharing can put your physical safety at risk.

Example: Posting your vacation plans publicly can alert potential burglars that your house is empty.

Scams and malware:

Scammers and hackers use social media to deliver scams and malware to users.

Example: You see an ad on Facebook about a giveaway, free prizes or game. You access a link that sends you to a fake website asking for your passwords or other information that is then stolen by the scammer.

Risks of Using Social Media:

Cyberbullying:

Negative interactions, including bullying and harassment, can occur.

Example: You receive mean comments on a picture you posted.

Inappropriate Content:

Exposure to inappropriate or harmful content.

Example: You come across a video with violent or explicit content.

Social Media and Influencers

Social influencers can be gamers, beauty, or fashion lifestyle vloggers who share their lives and opinions with millions of followers on platforms like Instagram, TikTok, and YouTube.

These popular online figures use social platforms not just to express themselves, but also to promote products and influence the behavior of their followers.

While they can be entertaining and inspiring, it's important to always be careful when following them, as they can easily shape your interests and hobbies or influence your attitude and self-esteem.

You should never forget that **not everything you see online is real or achievable** and that many influencers provide a polished version of their life to their viewers.

Negative Impact of Influencers

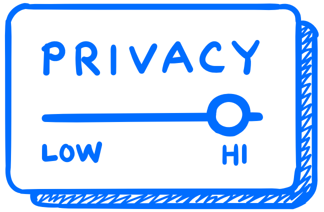
Not all influencers promote positive online behaviors. They may engage in **risky** or **inappropriate activities** and influence young audiences into mimicking their behavior or adopting **harmful habits**.

They can also have an **impact on your mental health** and contribute to **anxiety** and **stress**. Additionally, you need to be mindful of the potential for **online scams** promoted by less trustworthy influencers.

Tips for Safe Social Media Use:

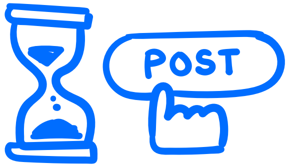
Parental Guidance: Keep parents informed about your activity and ask them to help you with settings. Seek help and inform a trusted adult about any suspicious activity or if you come across improper content.

Privacy Settings: Always use the highest privacy settings.



Be Wary of Requests: Never interact with strangers or accept friend or message requests from people you don’t know,

Think Before You Post: Always remember that posts are public and permanent.



Cyberbullying

Have you or someone you know ever experienced cyberbullying? How did it make you feel, and what did you do about it?

What is Cyberbullying?

Cyberbullying is the use of digital devices, sites, and apps to intimidate, harass, or harm someone. Cyberbullying can take many forms and can involve sending **hurtful messages**, **texts**, or **emails**, spreading false information about someone online or even **excluding someone** from an online group or game.

Forms of Cyberbullying:

Harassment: Repeatedly sending offensive messages.

Impersonation: Pretending to be someone else to cause harm.

Denigration: Sharing someone’s personal information without permission or posting harmful or false information about someone to damage their reputation.

Exclusion: Deliberately excluding someone from an online group or game.

Cyberstalking: intimidating or scaring someone by following them online.

Trolling: Provoking others into acting aggressively.

What to Do if You're Being Cyberbullied:

Opening Question: What would you do if you saw a friend being bullied online? How can you help them?

Bullies want attention, and you should never interact with them. They mean to intimidate and hurt you or the people around you.

Don't Respond: Do not engage with the bully.

Save Evidence: Keep screenshots or records of the bullying.

Be a Good Netizen: Never distribute harmful content about others.

Tell a Trusted Adult: Stay calm and report any incident to a parent, teacher, or another trusted adult.

Report and Block: Use the platform’s tools to report and block the bully.

Online Scams and Scammers

Opening Questions: Have you ever received a message or email from someone you didn't know asking for your personal information? What did you do?

Can you think of a time when you saw something online that seemed too good to be true? What did you do about it?

Common Scams:

Phishing Scams or Messages:

Scammers try to trick you into giving away personal information. They send emails, messages, or texts pretending to be from legitimate companies you know. These messages often direct you to fake websites that look like the real deal but harvest your personal information and passwords.

Example: You receive an email that looks like it's from your favorite game, asking you to enter your password.

Free Offers and Giveaways:

Scammers lure you with offers for free games or prizes to collect personal information or compromise devices with malware. Fake contests and giveaways often ask for a small payment to claim a non-existent prize.

Example: You see an ad for a free game download that installs malware on your device. You see an offer for in-game currency, items or cheats in exchange for money and data – The scammers never deliver on their promise.

Impersonation Scams:

Scammers pretend to be someone you know to gain your trust. They create fake profiles to steal your information money, stalk you online, and harass you.

Example: You get a message from someone pretending to be a friend, asking for your personal information.

Example: A scammer creates a fake Instagram account that looks similar to the account of an influencer you know. They post fake giveaways to steal your money and data.

AI Scams:

These scams involve the use of Artificial Intelligence to cause harm. This includes: fake messages and calls, deepfake videos (fake videos) that look like real ones, and phishing emails.

Example: You see a video that seems unbelievable about an influencer you know offering you a free iPhone in exchange for personal information and a small shipping fee.

How to Avoid Scams:

Be Wary of Unsolicited Messages: Don’t open emails and messages from people you don’t know. If something looks suspicious or sounds too good to be true, show it to a trusted adult. Don’t click on links you receive from strangers or in emails that ask to you act immediately – Requests to change a password or provide sensitive information.

Be Wary of Online Contests: Never enter contests and giveaways that ask for personal information. Always verify with an adult if the offer is real.

Check Sources: Always verify the source before providing any information or downloading apps. Use only official app stores and visit websites by typing the address yourself, instead of clicking on links in messages you did not request.

Keep Personal Information Private: Don’t share your address, phone number, school name, or passwords with people you don’t know online. Scammers can use this information to trick you or steal your identity.

Use Strong Passwords: Create strong passwords that are hard to guess. Use a mix of letters, numbers, and special characters. Don’t use easy-to-guess information like your birthday.

Enable Privacy Settings: Ensure that your social media and other online accounts have strong privacy settings to keep your information safe and prevent unwanted contact.

Report Suspicious Activity: If you see something suspicious or if someone tries to scam you, report it to the platform and tell an adult. This helps protect you and others.

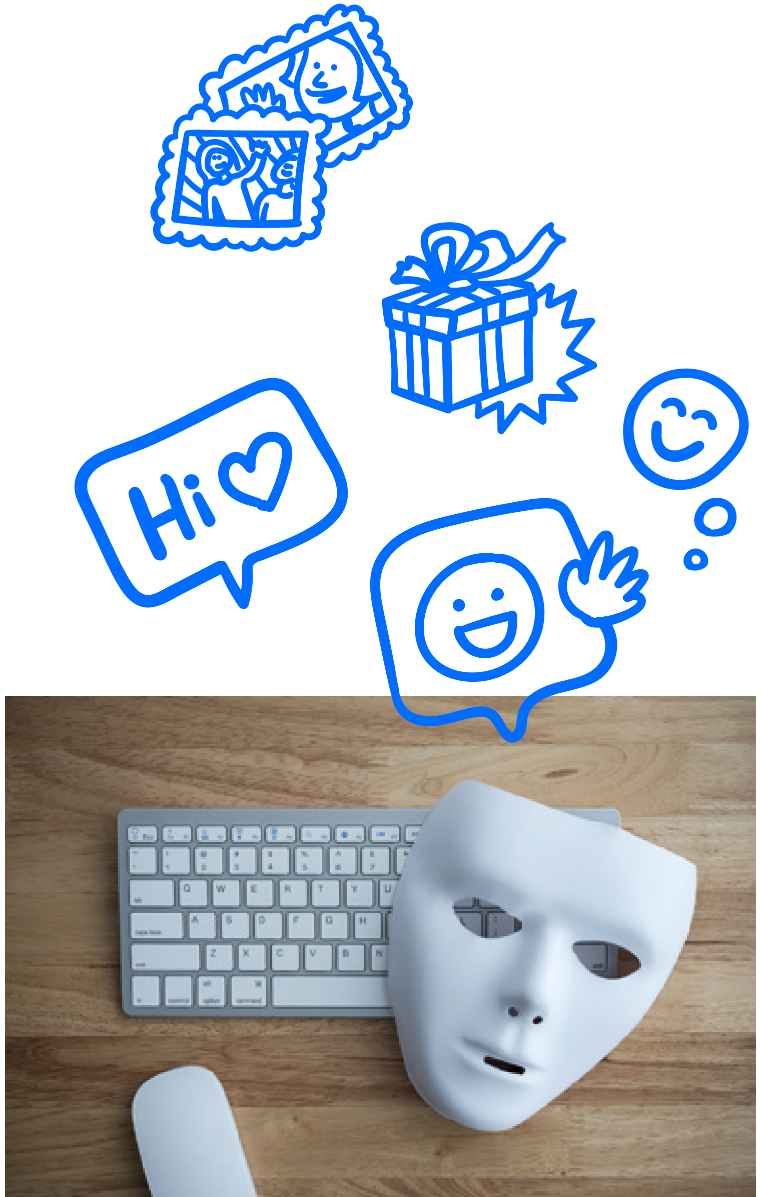
Protect Yourself Against Scams With Bitdefender Scamio!

Want an extra layer of protection to keep you safe online? **Try Bitdefender Scamio!** It's a cool tool that helps spot and block scams before they can trick you. Ask your parents to help you set it up so you can enjoy the internet safely and have more fun without worry. Stay smart, stay safe, and let Bitdefender Scamio be your superhero against online scams!

You only need to send Scamio texts, messages, links, QR codes, or images. Scamio will analyze them in a couple of seconds and tell you if they are part of a scam.

Social Media, Fake Identities and Strangers

Not everyone online is who they say they are. Some people create fake identities, pretending to be someone they're not. They might use pictures of other kids, seem very friendly, and make up stories to gain your trust. The individuals want to trick you into giving them personal information, like your address, phone number, Social Security number or even your parents' credit card details, and even share photos.



Understanding the Risks

Once the stranger has gained your trust, they might ask you to begin sharing **sensitive information** about you and your family. Some may try to use the information to bully or harass you, making you feel scared and upset. Others want your personal information to conduct identity theft crimes (use your social security number to take out a loan in your name).

A stranger you have befriended online might begin to ask you to **share indecent pictures or videos** – that can be used in ways you may not expect. They can share them with others without your permission, threaten and blackmail you in return for money, personal information, or other acts.

Young people are also targeted by individuals (usually, these perpetrators are much older than their target but claim they are of the same age or just a little older) who manipulate vulnerable youth into falling in love. They use the internet and social media to establish contact with victims and gather sensitive information. **In extreme cases, the individual will ask to meet you in person, putting your physical safety at risk.**

Red Flags

Unsolicited contact over a long period of time to gain confidence

Requests for **sensitive** information

You are asked to keep your relationship and conversations **a secret**

You **feel isolated** from friends and family

The perpetrator **acts aggressively** or **violently** if you do not answer their messages and threatens you

You receive **inappropriate requests** such as sharing pictures and videos of you

You are **forced** to perform activities you don't consent to

Staying Safe

When you talk to strangers online, whether in a game, on social media, or on a forum, you can't always tell if they are telling the truth about who they are and their real intentions.

Always think twice before sharing any pictures online

Make sure you **never reveal personal information** like your school, phone number, home address, or where you hang out.

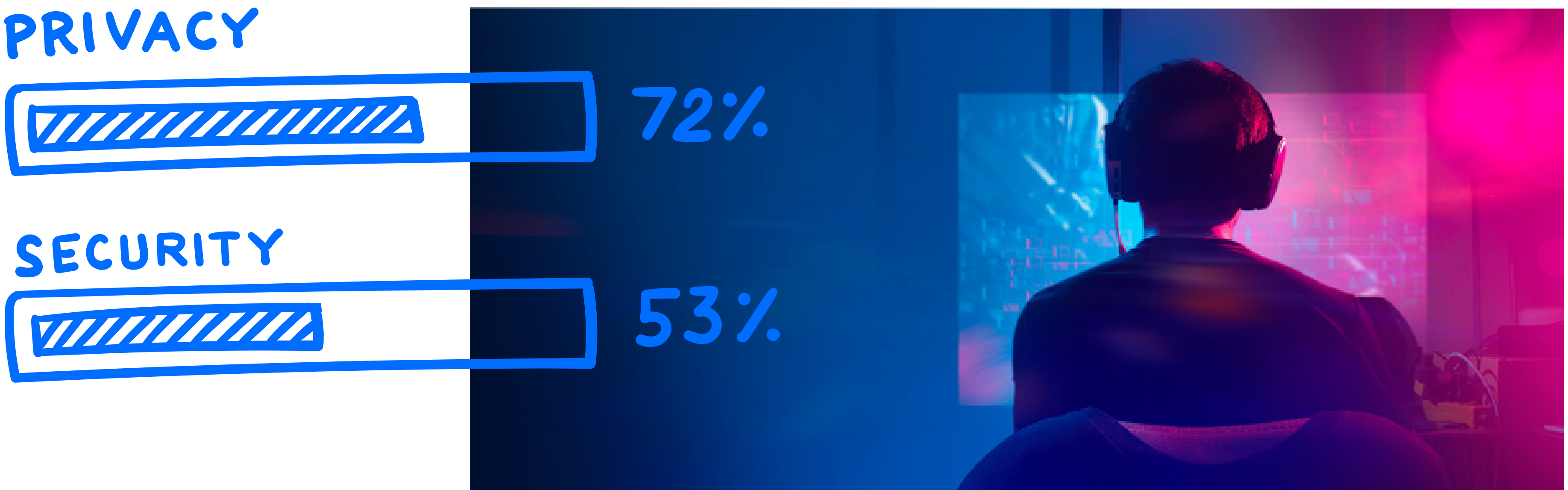
Keep your social media accounts private and only share pictures with people you know and trust.

Use the report features on the platform and immediately **tell a trusted adult** if something online makes you uncomfortable or if someone you don't know tries to contact you or make any inappropriate requests.

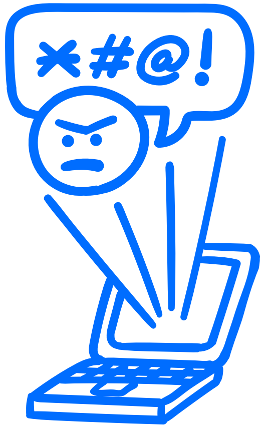
Online Gaming

What are your favorite gaming platforms and what are some steps you take to make sure your online gaming experience is safe and fun?

Popular gaming platforms like Roblox, Fortnite, Minecraft, and Among Us have millions of young users who enjoy building, competing, and socializing in these digital spaces. Communicating with other players through chat and voice features adds to the social experience, allowing kids to make new friends and collaborate on in-game tasks.

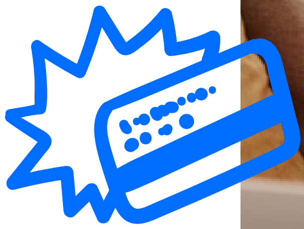


The popularity of online gaming also comes with certain risks that you need to be aware of, including:



Online Harassment: Players may encounter bullies and bad behaviors.

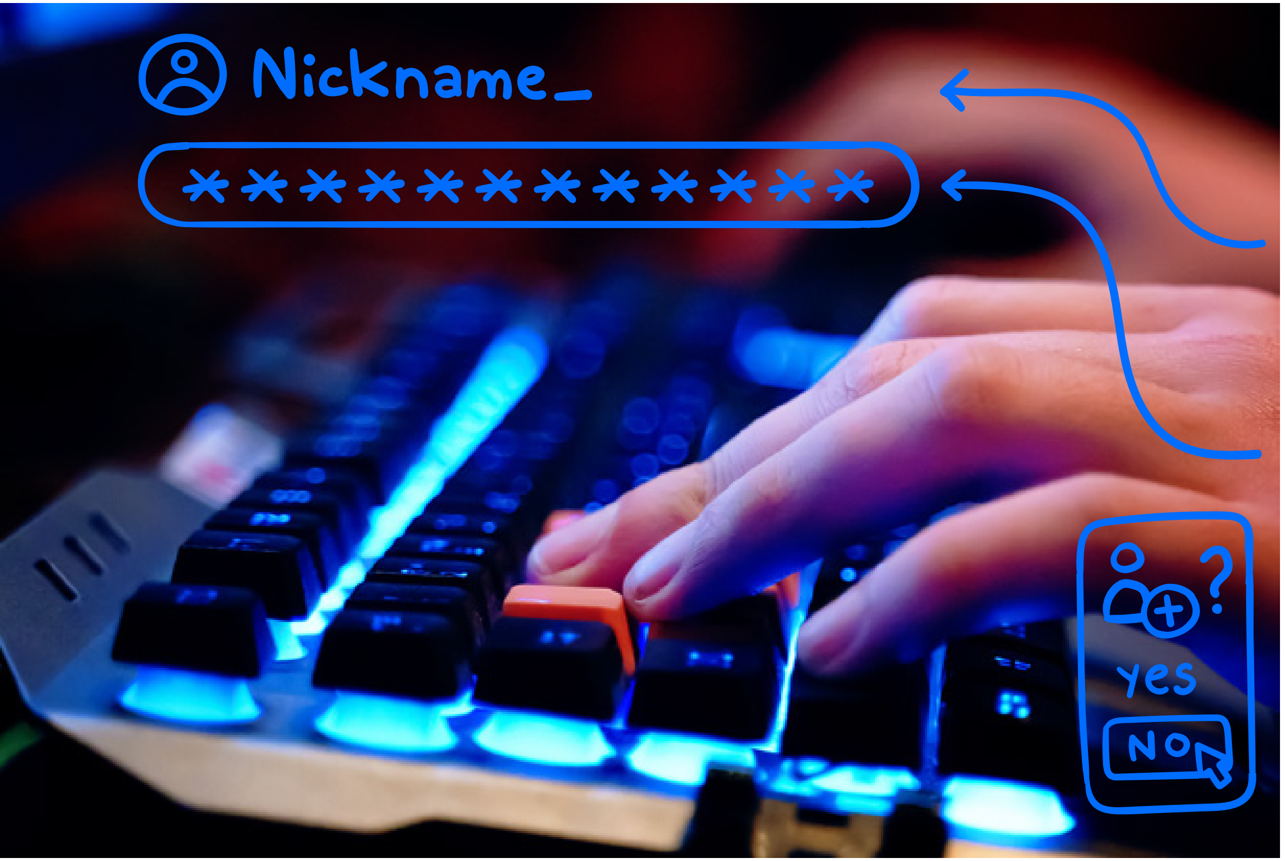
Exposure to Unsuitable Content: Some games may have content that is not suitable for all ages. You encounter players who use bad language or make inappropriate comments or share unsuitable videos, photos and websites



In-Game Purchases: Players are spending real money on in-game items. Buying virtual items with real money without realizing it.

Online Predators: Adults use gaming platforms to build fake relationships with younger players, causing emotional and physical harm.

Scams: Scammers may trick you into giving away personal information, account details, money and passwords.



Best Practices for Safe Online Gaming

Don't Share Personal Information:

Avoid sharing personal details with other players. Use Nicknames or usernames that don’t reveal your real name

Use Strong and Unique Passwords:

Don’t use the same password for multiple games or accounts.

Adjust Your Privacy Settings and Limit Friend Requests:

Set your gaming profiles to private to control who can see your information and interact with you. Only Accept Friend Requests from people you know in real life.

Communicate Safely:

Be careful when using voice chat. Don't reveal personal information or details that could identify you. If possible, use in-game messaging systems that have moderation and reporting features.

Limit Playtime:

Agree on a reasonable amount of time for gaming to ensure it doesn't interfere with your homework, sleep, or other activities. Make regular breaks to prevent fatigue and maintain a healthy balance.

Report and Block Abusive Players:

Use the game's tools to report and block any players who behave inappropriately.

Digital
Safety Quiz

Question 1: What is a digital footprint?

a) A trail of physical footprints you leave when walking
b) The trail of data you leave behind when you use the internet
c) A type of social media account
d) A game played online

Question 2: Why is it important to safeguard your personal information online?

a) To prevent identity theft
b) To avoid scams
c) To protect your privacy
d) All of the above

Question 3: Which of the following is NOT an example of personal information?

a) Your full name
b) Your favorite color
c) Your home address
d) Your phone number

Question 4: At what age do most social media platforms allow users to create an account?

a) 10 years old
b) 13 years old
c) 16 years old
d) 18 years old

Answers:
Q1. b) The trail of data you leave behind when you use the internet
Q2. d) All of the above
Q3. b) Your favorite color
Q4. b) 13 years old

Question 5: What should you do if you are being cyberbullied?

a) Respond with mean messages
b) Ignore it and do nothing
c) Save evidence and tell a trusted adult
d) Share your password with the bully

Question 6: What is a common type of scam targeting kids?

a) Free offers for games or prizes
b) Invitations to birthday parties
c) Homework-help websites
d) Online tutoring sessions

Question 7: Which of the following is not a safe practice for online gaming?

a) Sharing your personal information with other players
b) Threatening other players in chatrooms
c) Clicking on every link shared by other players
d) Buying virtual items without asking permission

Answers:
Q5. c) Save evidence and tell a trusted adult
Q6. a) Free offers for games or prizes
Q7. b) All of the above

Thank you.

Trusted.
Always.