



Top 10 Online Safety Tips



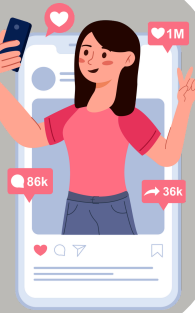
1

Don't Share your personal information



2

Think carefully about what you post



3

Only talk to people you know



4

Only accept friend requests from people you know



5

Use Privacy settings on all your social media accounts

6

Not everyone online is who they say they are



7

Never share your password



8

Only share images you'd be comfortable with your family and friends seeing



9

Report inappropriate content immediately



10

Don't meet up with anyone you have only met online



TAKE THE QUIZ



Questions



1. What is the definition of "Online Exploitation"?

- A. When someone uses the internet to build trust with a child to eventually manipulate them
- B. When a computer virus deletes your homework.
- C. When you accidentally buy something online.
- D. Spending more than 4hr a day on social media platforms.

2. Which platforms can exploitation happen on?

- A. Only social media
- B. Only gaming sites
- C. Anywhere people can message each other
- D. Only email

3. What is a Key Sign that a child might be experiencing 'Online Grooming'?

- A. Showing a sudden interest in outdoor sports and offline activities.
- B. Secretive behavior about online activity or unexplained new gifts and money.
- C. Asking parents for help when they encounter a technical error on their tablet.
- D. Refusing to share their school login password with their best friend.

4. What is the safest way to handle friend requests on social media?

- A. Accept requests only from people they know in real life
- B. Accept any request as long as the person has a profile picture of people of similar age
- C. Accept everyone but set the account to "public" so parents can see everything
- D. Wait three days before accepting a stranger's request to see if they are a bot.

Questions



5. Which of the following is a "Healthy Online Habit" for families?

- A. Allowing children to use devices in their bedrooms with the door locked.
- B. Keeping conversations about online safety open and regular.
- C. Unlimited use of social media
- D. Checking a child's messages secretly without them knowing.

6. If you suspect online exploitation, what you should do?

- A. Save evidence like screenshots.
- B. Visit the website www.cybertipline.org to report
- C. Tell your parents about the situation
- D. All of the above

7. Why should you use Two-Factor Authentication (2FA)?

- A. To make the internet run faster on your devices.
- B. To add an extra layer of security to prevent scammers from accessing accounts.
- C. To limit the amount of time a child can spend on a gaming platform
- D. To block all advertisements and pop-ups while browsing.

8. What is a primary danger regarding online gaming chat features?

- A. They use up too much data on the family's internet plan.
- B. They allow strangers to contact children and build trust to start conversations.
- C. They make games too difficult for younger children to play.
- D. They automatically share your home address with everyone in the game.

Questions



9. An email from "Roblox Support" says your account will be deleted unless you click a link to verify your password. What should you do?

A. Click the link immediately to ensure you don't lose your game progress.

B. Ignore the email and visit the official website directly by typing the address in your browser.

C. Reply to the email with your password to prove you are the real owner.

D. Forward the email to all your friends to warn them about account deletions.

10. Which organization can you contact to report that a child is being exploited or approached inappropriately online?

A. The National Center for Missing and Exploited Children (NCMEC).

B. Report to the gaming/social media platform where the incident happened

C. Local Law Enforcement

D. All of the above



Have more questions or need more great tips and guidelines?

Follow us on www.protectall.org and download the full guide!



Top 10 Online Safety Tips



THE IPA SHIELD

A COMPREHENSIVE GUIDE TO ONLINE SAFETY FOR PARENTS

Protecting Your Family in the Digital Age

[Download here](#)

**Click the link or
scan the QR code!**





Question 1: A

Online Exploitation involves using digital platform to build relationships for the purpose of coercion and/or harm.

Question 2: C

Anywhere people can message each other

Question 3: B

Behavioral changes like secrecy and receiving items from unknown sources are major red flags for grooming.

Question 4: A

Should limit their circles to known individuals and set profile settings to "friends only".

Question 5: B

Communication is the foundation of safety; kids report problems more often if they feel supported.



Question 6: D

Do not confront an offender as it can be dangerous. Instead, save evidence and report to the platform or law enforcement

Question 7: B

2FA adds an extra layer of protection to keep accounts secure from scammers

Question 8: B

Chat features are often used by predators to reach targets and start grooming.

Question 9: B

Visit official sites directly. Companies will never ask for passwords via messages or emails

Question 10: D

All of the above