THE IPA SHIELD

A COMPREHENSIVE GUIDE TO ONLINE SAFETY FOR PARENTS

Protecting Your Family in the Digital Age

International Protection Alliance
SAFEGUARDING FUTURES GLOBALLY

NEXT PAGE

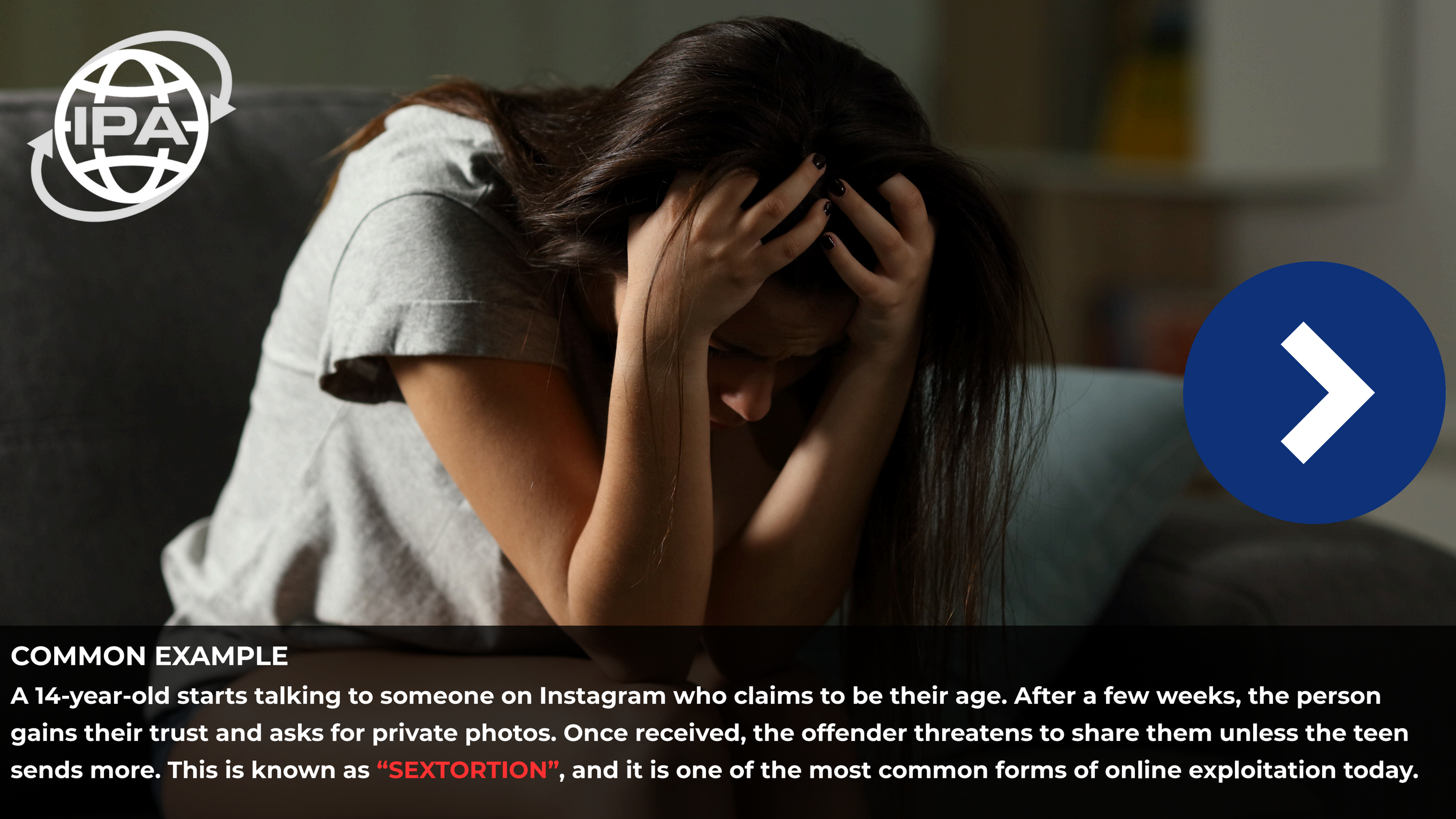
Kids spend more time online than ever, learning, playing, chatting, and exploring. The internet offers great opportunities, but it also carries risks. One of the most serious is online exploitation, where someone uses the internet to trick, manipulate, or harm a child. This booklet helps parents understand how exploitation happens, what warning signs to look for, and what steps to take to protect children online. You do not need to be a tech expert. Staying informed and having open conversations with your child can make all the difference.

DEFINITION: Online Exploitation *noun*

(on-line ex-ploi-ta-tion)

Online exploitation happens when someone uses the internet to build trust with a child or teen and then manipulates, coerces, or harms them for sexual, financial, or emotional reasons. Offenders may pretend to be other kids, use fake profiles, offer gifts, or slowly groom their targets over time. Exploitation can occur on social media, chat rooms, gaming platforms, and even in group messaging apps.

(Definition provided by IPA)



COMMON EXAMPLE

A 14-year-old starts talking to someone on Instagram who claims to be their age. After a few weeks, the person gains their trust and asks for private photos. Once received, the offender threatens to share them unless the teen sends more. This is known as **“SEXTORTION”**, and it is one of the most common forms of online exploitation today.

Tips for Parents:

- Talk to your child about what online exploitation is and why it is dangerous. Use simple, honest language.
- Remind them that anyone online can pretend to be someone else.
- Teach them not to share personal details, photos, or videos with people they only know online.
- Keep communication open and judgment free. Let them know they can come to you if something feels wrong.
- Review privacy settings on apps and limit who can message or follow your child.
- Keep devices in shared spaces when possible.
- If you suspect exploitation, save evidence such as messages, usernames, and screenshots, and report it to the platform or law enforcement right away.

SOCIAL MEDIA SAFETY

Social media is one of the most common ways predators and scammers connect with kids. Even with privacy settings on, strangers can still send messages, friend requests, or join mutual groups to gain access.

COMMON EXAMPLE

A 12-year-old accepts a friend request from someone pretending to be a classmate. Over time, that person starts manipulating and “GROOMING” the child. Online grooming is when someone uses the technology or the internet to build a relationship with a young person, with the intention of tricking, pressuring or forcing them into doing something sexual, like sending images or videos of themselves.

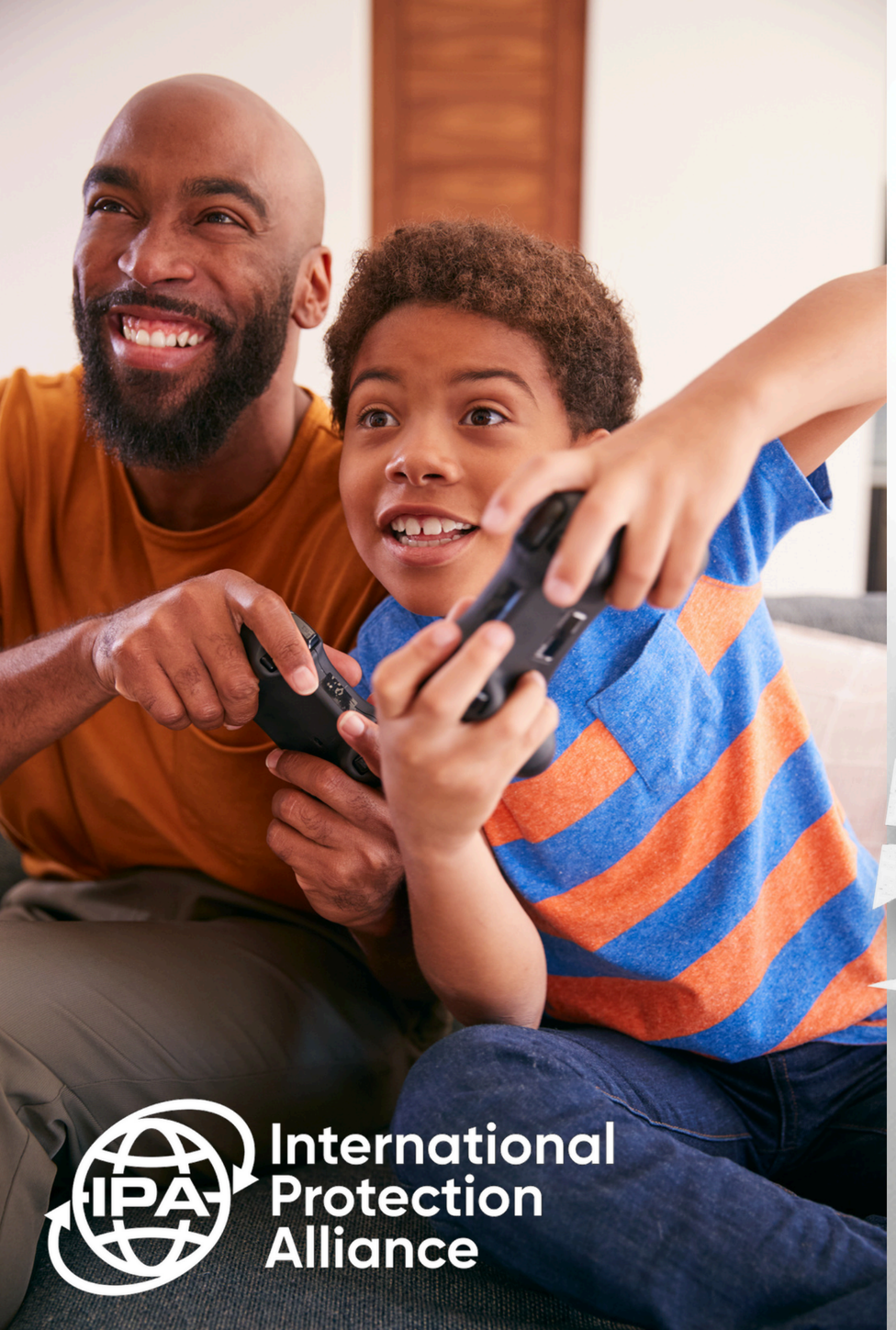
Tips for Parents:

- Review privacy settings with your child and set profiles to “friends only.”
- Encourage them to accept requests only from people they know in real life.
- Remind them never to share their location, school, or daily routine online.
- Check their friend lists together and remove unfamiliar contacts.
- Talk about what is appropriate to post and what should stay private.
- Know the Signs of Grooming; Be alert to behavior changes, such as secretive behavior about online activity, increased time online, especially late at night, unexplained new gifts, money, or items, and withdrawn, anxious, or aggressive behavior.

International Protection Alliance

SAFEGUARDING FUTURES GLOBALLY

GAMING SAFETY



Online games are fun and social, but the same chat features that help players connect can also allow strangers to contact children. Some predators use games to start conversations and build trust.

Tips for Parents:

- Know what games your child plays and whether they include chat features.
- Use parental controls to limit who can contact your child or to block strangers.
- Remind them never to share personal information or photos while gaming.
- Encourage them to tell you right away if someone says or asks anything uncomfortable.

“Phishing” happens when scammers send fake messages pretending to be a company or friend in order to trick people into sharing passwords, account details, or downloading harmful files.

COMMON EXAMPLE:

Your child receives an email from “Roblox Support” saying their account will be deleted unless they verify their password. The link leads to a fake website that steals their login information.

Tips for Parents:

- Teach kids not to click on links from messages they were not expecting.
- Remind them that companies will never ask for passwords through messages.
- Turn on two-factor authentication (2FA) on accounts they use.
- Visit official websites directly instead of following links.

HEALTHY ONLINE HABITS

Creating a culture of safety online starts with communication and clear boundaries. Kids are more likely to tell parents about online problems if they feel supported and not judged.

Tips for Parents:

- Keep conversations open and regular. Ask what your child enjoys doing online.
- Set clear rules about screen time and device use.
- Encourage breaks from screens and promote offline activities.
- Keep computers and gaming consoles in shared spaces when possible.
- Use parental tools to monitor new apps or messages without invading privacy.


IPA Online Safety Checklist
Talk openly with your child about online safety.
Keep social media accounts private.
Teach kids not to share personal information or passwords.
Review friend lists and privacy settings.
Install antivirus software and keep devices updated.
Use parental controls where available .
Encourage your child to tell you if something online makes them uncomfortable.

If you suspect that your child is being exploited or approached inappropriately online:

- Save all evidence, such as screenshots, usernames, messages, and links.
- Do not confront the offender directly. Report the account or message to the platform immediately.
- Contact law enforcement or the National Center for Missing and Exploited Children (NCMEC).
    - Website: **www.cybertipline.org**
    - Phone: **1-800-THE-LOST (843-5678)**

For more tips, resources, and educational materials, visit **www.protectall.org**