SH1ELD Tech Cyber Safety Blog

*A brief guide to be a secure and aware citizen in Cyber space, by understanding the Do’s and Don’ts of Digital World you can stay safe and secure.*

**SOCIAL MEDIA**

1. **Keep Personal Information Professional and Limited**
2. **Keep Your Privacy Settings on and Practice Safe Browsing**
3. **Make Sure Your Internet Connection is Secure.**
4. **Keep Your Antivirus Program Up to Date**
5. **Be Careful What You Download**
6. **Choose Strong Password**
7. **Make Online Purchases from Secure Sites only**
8. **Be Careful What You Post**
9. **Be Careful Who You Meet Online**

**FINANCIAL TRANSACTIONS**

1. **Make sure personal banking information is accessible to only you.**
2. **Never share personal banking information like:**

**OTP, CVV, Login Credentials, Credit/Debit Card Details, Date of Birth, Name or any such information over a Phone call, Text message, Email etc.**

1. **Use Secure Internet Connection while making online Financial Transactions.**
2. **Always check whether the Payment Gateway and website is Secure or not (https)**
3. **Never do Online Banking on Public WIFI.**
4. **Make sure you stay updated and connected with latest cyber threats and cybercrimes in the market.**

**INTERNET SAFETY FOR TEENAGERS**

##  Why internet safety matters

Teenagers use digital technologies for everyday activities like keeping in touch with friends on [social media](https://raisingchildren.net.au/teens/entertainment-technology/digital-life/social-media), relaxing and doing schoolwork. They also go online to look for support for physical or mental health problems, and sometimes to experiment with different ways of expressing themselves.

Because they’re online so much without your supervision, teenagers **need to be able to identify acceptable and unacceptable online content independently**. They also need to know how to behave respectfully online and avoid online risks.

## Internet safety risks for teenagers

There are four main kinds of internet risks for teenagers.

**Content risks**
For teenagers, these risks include coming across material that they might find upsetting, disgusting or otherwise uncomfortable, especially if they encounter it accidentally. This material might include:

* [pornography](https://raisingchildren.net.au/teens/entertainment-technology/pornography-sexting/pornography-talking-with-teens) or sexually explicit content in music videos, movies or online games
* real or simulated violence
* hate sites
* terrorist sites
* fake news that seems believable
* harmful user-generated content like sites about drug use, self-harm, suicide or negative body image.

**Contact risks**
These risks include coming into contact with adults posing as children online, strangers who persuade teenagers to meet them in real life, and online scammers.

**Conduct risks**
Conduct risks include behaving in inappropriate or hurtful ways, or being the victim of this kind of behaviour. Examples include:

* [cyberbullying](https://raisingchildren.net.au/teens/entertainment-technology/cyberbullying-online-safety/about-cyberbullying)
* [sexting](https://raisingchildren.net.au/teens/entertainment-technology/pornography-sexting/sexting-teens)
* misusing people’s passwords and impersonating people online
* making unauthorised purchases using other people’s financial details
* creating content that reveals information about other people
* having trouble regulating online time, which can develop into problem internet use.

**Contract risks**
Contract risks include teenagers signing up to unfair contracts, terms or conditions that they aren’t aware of or don’t fully understand. As a result, teenagers might:

* be open to identity theft or fraud
* get inappropriate digital marketing messages or scam emails
* have their personal data collected from apps and devices like fitness trackers.

## Protecting teenagers from internet safety risks

Your child is probably an independent internet user now, but you can help your child keep building the skills and knowledge they need to identify and manage internet safety risks.

Here are some basic things you can do to protect your child from internet safety risks:

* Create a family media plan. It’s best to negotiate your plan with your child. Your plan could cover things like screen-free areas in your house and what online behaviour is OK.
* Talk with your child about upsetting and inappropriate content. If you can talk with your child in an open and non-judgmental way, they’re more likely to talk with you if they come across something disturbing online or have a bad online experience.
* Stay in touch with what your child is doing online and how much time they’re spending online. This will help you to spot when your child might be having problems.
* Ask your child to ‘friend’ you on social media. Younger teenagers might be OK with this, but older teenagers might prefer not to friend you.
* Encourage and remind your child to explore and use the internet safely. For example, it’s OK to remind your child to check privacy settings.
* Find out how to make complaints about offensive or illegal content

Technical internet safety tools like **internet filters can actually increase risk** for children over 14 years. If children are using filters at this age, they might not be developing the skills they need to avoid disturbing content. They might take risks either accidentally or on purpose when they use the internet in unfiltered environments.

## Identifying and managing internet safety risks with teenagers

It’s important to **help your teenage child manage internet safety risks**. This lets your child build digital resilience, which is the ability to respond positively and deal with risks they come across online.

You can do this by:

* being a role model for healthy internet use
* talking with your child about online content and behaviour
* reminding your child about privacy and personal information
* teaching your child about online purchases.

**It’s all about building your child to become a responsible digital citizen.**

## Being a role model for internet use

All children – including teenagers – do as you do, so being a role model for your child is a powerful and positive way to guide your child’s behaviour when it comes to internet use.

You can be a role model for safe and healthy screen use by using digital media and the internet in the way you want your child to use it. For example, you might keep internet-connected devices out of bedrooms, avoid using your phone during mealtimes, or balance screen use with other social and recreational options.

It’s also good to model positive technology use like phoning friends and family and sending supportive messages.

## Talking about online content

Talking openly about your own digital media and internet use and encouraging your child to do the same will **help your child feel they can talk to you if they have a bad experience online**.

You can get your child talking by asking them to explain the apps, games and content they’re interested in. You might say, ‘Snapchat posts disappear quickly, but a screenshot can capture what’s been said. Is that right?’ Or ‘Talk me through the differences between YouTube and TikTok’.

It’s good to encourage your child to develop a sense of what they like and don’t like online and to defend their choices with friends. For example, you could say, ‘It’s great that you chose not to get involved in that online argument’.

Talking about **online hoaxes and fake news** with your child will help them develop the ability to tell whether the child is Digitally aware.

This is all part of digital and media literacy.

## Taking care with privacy, personal information and personal safety

You can help your child look at and **choose appropriate privacy, location and safety settings** on devices, programs and social media, and talk about why this is important.

It’s also important for your child to be careful about sharing personal information. Remind your child not to give out their name, address, date of birth or other identifying information to people they don’t know in person and not to send or post images to people they don’t know.

Some useful website links to stay connected and updated in cyber space by becoming a digitally aware citizen.

***YOU CAN REGISTER YOUR ONLINE COMPLAINT HERE AT GOVERNMENT PORTAL:***

* Are you a victim of cybercrime? Register your complaint at “National Cyber Crime Helpline” [www.cybercrime.gov.in](http://www.cybercrime.gov.in/)

**OFFICIAL COMPUTER EMERGENCY RESPONSE TEAM INDIA**

https://www.cert-in.org.in

**CYBER SWACHHTA KENDRA** – Botnet and Malware Cleaning

<https://www.cyberswachhtakendra.gov.in>

**CYBER SECURITY VOLUNTEER**

https://cybervolunteer.mha.gov.in

**MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY**

https://www.meity.gov.in

***Any form of illegal changes and modification will lead to Copyright Infringement,***

***SH1ELD Tech Copyright.***