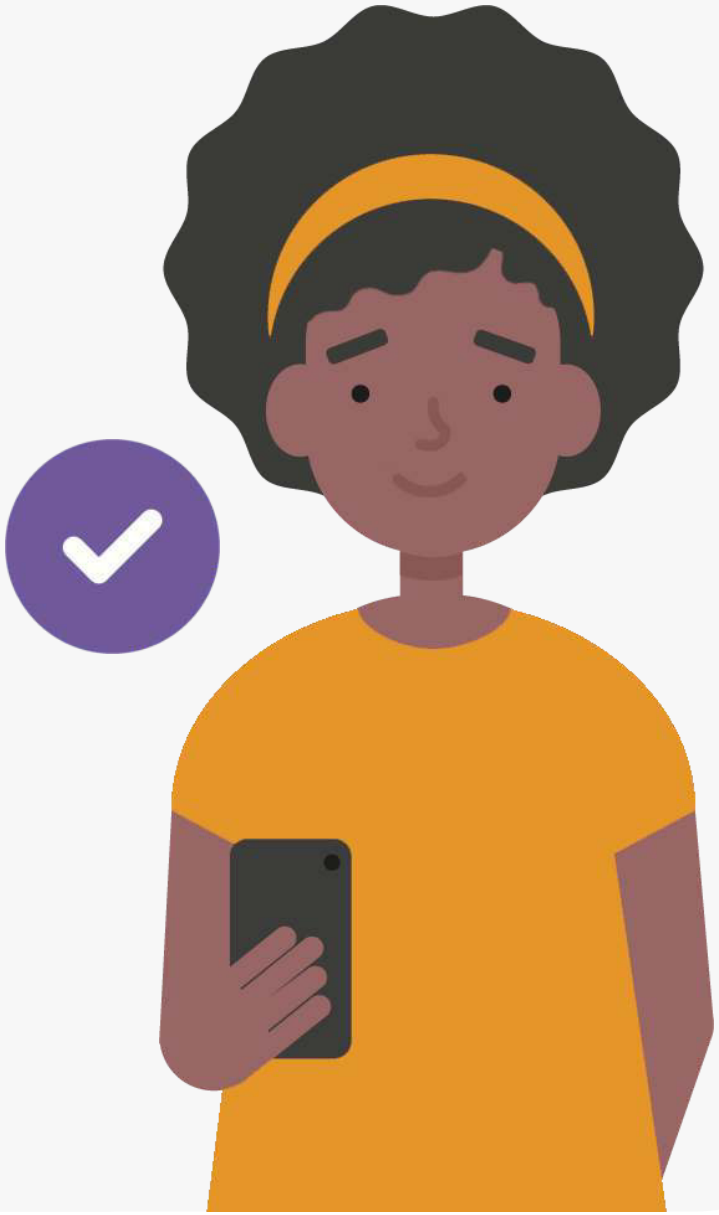
internet matters.org

Tackling online scams

Tips to spot the signs and get support



Jump to...

3 types of common online scams

Phishing →

Financial →

False promises →

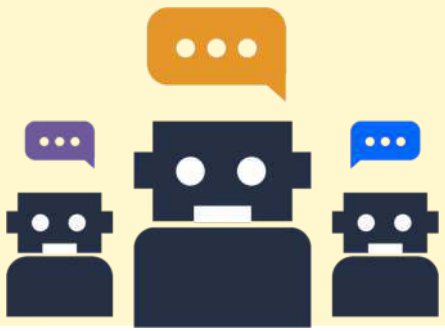
Phishing

Phishing is when a cyber criminal tries to get personal information from someone or influence them to complete a task. Examples include:

- Posing as a known or potential friend through social media or email to gain trust from the victim and steal their personal information.

- Sharing a URL or app download link that allows criminals to gain access to a device or personal information.

- Acting as web support or posing as someone they're not in public virtual meetings, gaining access to private information.



Financial

From get-rich-quick schemes to form-jacking, online financial scams are rampant. They can cause huge loss and long-term impacts. Examples include:

- Courses promising users a large income without a lot of effort (popular among cryptocurrency, NFTs and even copywriting).

- Fake shopping sites or shopping sites with lax security, allowing form-jacking where cyber criminals can steal the payment information you enter.

- Fake competitions, scholarships and more that require payment to enter, only for the money to be stolen and criminals to disappear.

False promises

Promises of weight loss and free items or services like tech support are often scams aimed at getting money or information. Examples include:

- Diet pills, protein powders and other ‘health’ products prey on social media pressures, rarely providing the service they claim

- Pop-ups or ads that claim your device or computer are under attack are often a type of phishing scam, promising protection but likely installing malware on your device.

- Ads, messages or calls providing forms or instructions to fix it often result in stolen information, financial loss or installed malware.

Learn more...

Return to menu

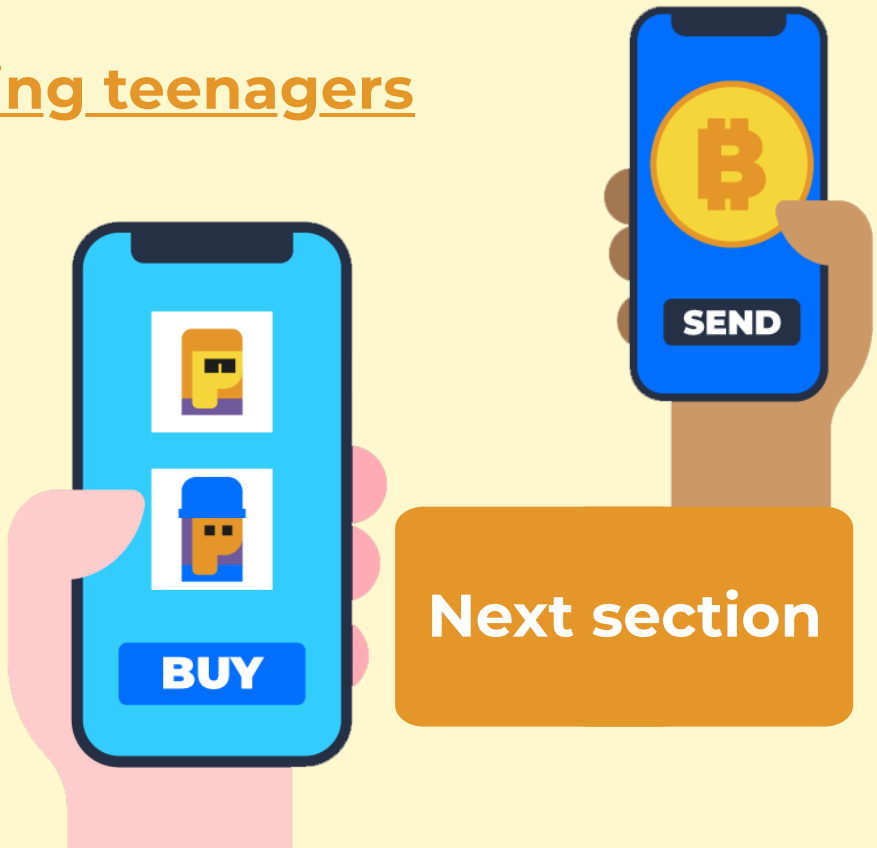
Stay informed about online scams to help keep your child safe.

Financial scams and the impacts on young people

Common online scams targeting teenagers

Social media scams

Types of cyber attacks



Next section

The signs to look for

What's the source? →

Is your personal information safe? →

Does it look trustworthy? →

What's the source?

Whether it's on social media, in a video game or through email or messaging, it's important to check that the source is reliable.

- If a friend or follower sends a link from their account, verify it was in fact them. Use a different service and ask!

- See a link from a random internet user? Go to the website a different way instead of clicking on the link or use search engines to check its trustworthiness.

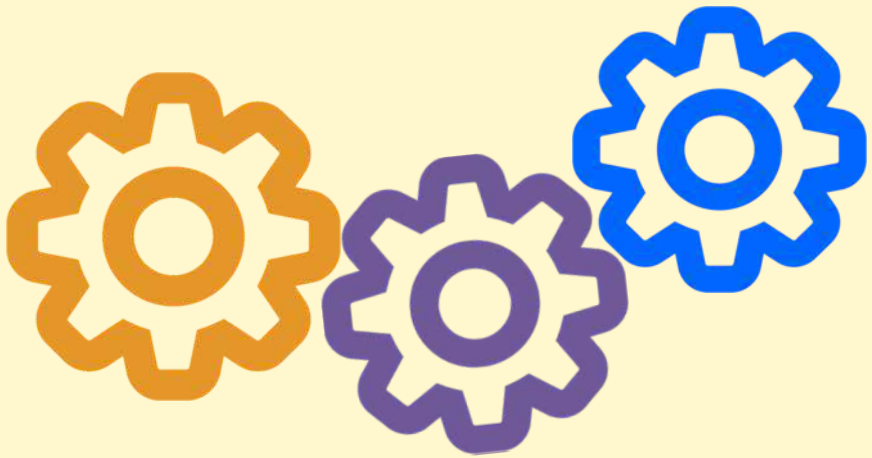
- Remember that official logos do not mean something came from that company!

Is your personal information safe?

If anyone online asks for personal information, payment details or any sort of action, be sure to confirm that it's real before doing so.

Platforms will not send emails to ask this kind of information, and no one on social media or in-game should either.

Use different passwords for your accounts, use anti-virus software and, if something feels off, ask around and do a little research.



Does it look trustworthy?

While many online scams have become more sophisticated, there are some tell-tale signs to look out for that could suggest a scam:

- Spelling and grammatical errors
- Few reviews or low ratings of an item
- Comments from others calling something a scam
- Poor design and layout
- Expensive items for a very low price

If something feels off or like it’s too good to be true, make sure you take time to look into it before clicking links or giving details.

Learn more...

Return to menu

Stay informed about identifying online scams and misinformation to keep your child safe.

Online critical thinking guide

Fake news and misinformation hub

Find the fake interactive quiz

Summary of types of fake news

Next section

How to tackle online scams

Stop communication →

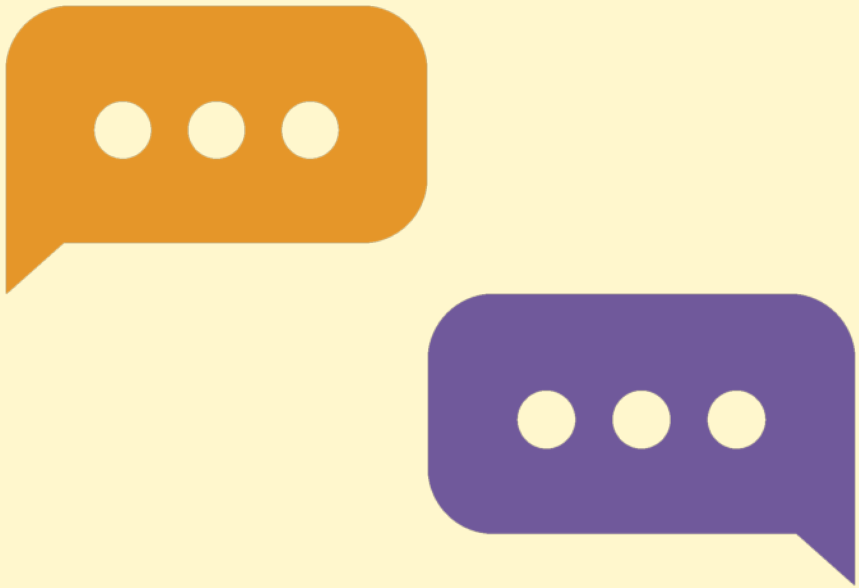
Report the scam →

Seek support →

Stop communication

Once you realise something is a scam, stop talking to the scammer.

Don’t call them a scammer or apologise. Simply stop all contact and use block functions where possible.



Report the scam

Help stop the scammer from targeting others by reporting them where necessary.

- Forward phishing emails to phishing@gov.uk and phishing texts to 7726.

- Report scam ads to the **Advertising Standards Authority (ASA).**

- Scams and cyber crime should also be reported to **Action Fraud** (or the police in Scotland).

- Report on the platform (including search engines) it came from as well.

Report the scam

If you have been financially impacted, you may need to report to **Action Fraud** police as well. Save screenshots of messages and any other proof in case you need it.

Financial scams involving your credit or debit card should be reported to the relevant company or bank as well to help make them aware.

Seek support

You don't need to deal with the impacts of scams by yourself.

Scams may impact you financially, requiring support from your bank or credit card company, but they can also affect your mental health.

Talk to friends and family or mental health services for personal support.

Learn more...

Return to menu

Stay informed about how to tackle online scams to help children stay safe and have fun online.

How to tackle online scams

What is cyber security?

How a strong password protects from data breaches

Keeping kids safe: Phishing and ransomware

Finish