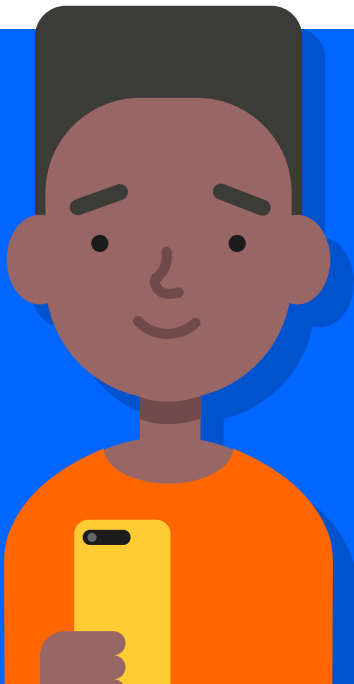devices**.now**

internet matters.org

Online Safety Guide

Get simple tips to make your time online safer ▶▶

See advice from **Internet Matters** and **DevicesDotNow** to help you enjoy the internet safely.

Here are a few things you can do to stay safe online

1 **Protect your personal information online**

Your personal information is anything that can be used to identify who you are like your address, your email address or phone number. **This information can be used by some people to scam you or to create fake accounts in your name.**

To keep it safe, only share this information with sites that are reputable and when absolutely necessary. If you are talking to someone online that you don't know, it's best not to share this at all unless you know how this information will be used.

2 **Manage privacy settings on apps**

If you are using social media sites like Facebook or WhatsApp to connect with your family and friends, **it's important to check your privacy settings.** These control who can see what you are posting on your account. They can also control what information on your account is public (for everyone to see) and private (only you can see).

To manage what you share safely, review these settings regularly to give you the confidence that you are sharing things with the people you want to.

To learn how to use privacy settings on a range of popular apps, visit internetmatters.org/controls
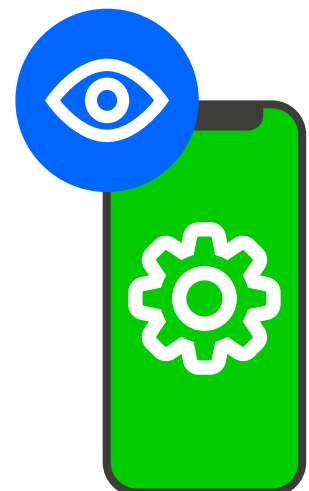
3 Spot the difference between what's fake and what's real

With so many people sharing information online, at times **it can be hard to see the difference between what's real and what is fake online.**

Sometimes people may share something with you that they think is real but it's not. Scammers may also send you fake emails pretending to be from your bank or other organisations to collect your personal information. Or you might accidentally visit a fake website set up to pretend to be real to scam you.

To check if something is real online you should:

- Check the source of the information

- Do a search on the organisation or person it's come from to see if they are real

- Check if the web address looks suspicious

- If it's fake, report it, delete it, and don't share it.
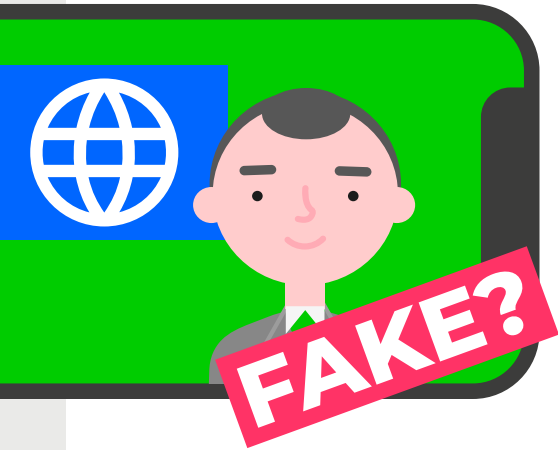
4 Manage your money safely

To keep your financial information safe online, when shopping or banking, **make sure that you are using a secure website before giving your personal details.**

To check this, **look for a padlock symbol in the browser bar** and make sure the web address begins with 'https' rather than 'http'. The 's' stands for secure. Try to **buy from companies you know**. Avoid using a public Wi-Fi connection to avoid hackers getting your details.

To learn more about keeping your money safe online visit moneyadviceservice.org.uk

www.internetma
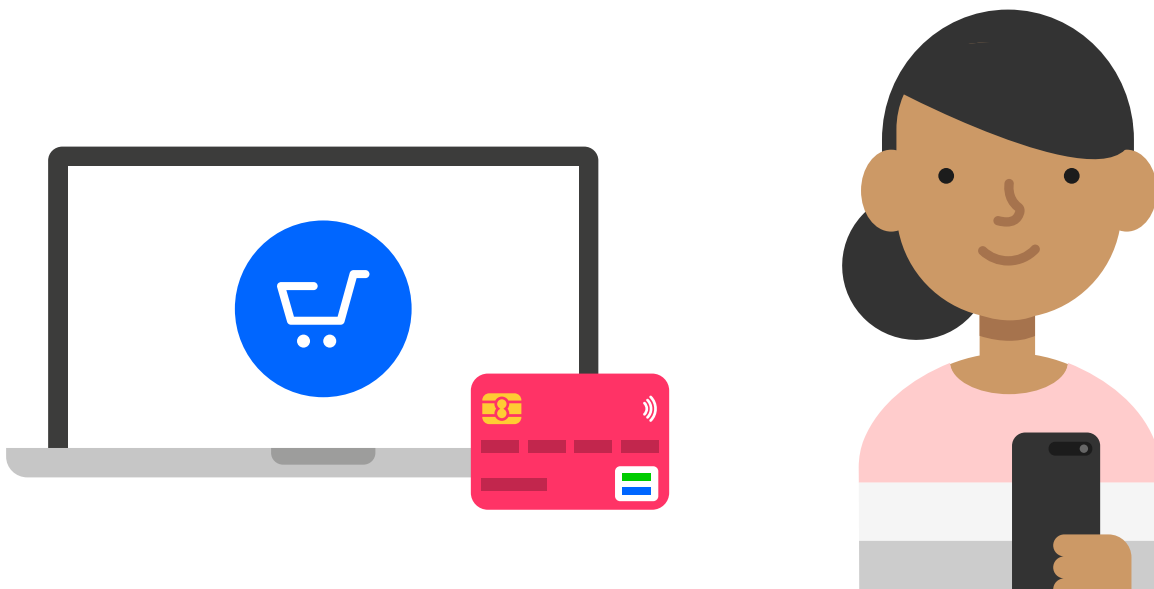
5

Got a problem? Know where to get help

Most popular apps you use will have a way for you to report or block someone or something that may upset you on their platform. Find out how to best use these tools so you can deal with online issues as quickly as possible. For more support on how to report issues visit reportharmfulcontent.com

If you've seen something online that contains indecent images of children, please make a report to one of CEOP's Child Protection Advisors at ceop.police.uk. They will take the necessary steps to address the incident.

If you receive an email that you think looks at all suspicious you can forward it to report@phishing.gov.uk. You can also report fraud which includes online or internet crimes, using the Action Fraud reporting tool - actionfraud.police.uk

Need to protect a child online too?
Here are a few extra things you can do to keep them safe

1. **Support them online** by having regular check-ins with them about what they do online. This will give you an idea of what advice and guidance they need to stay safe.

2. **Agree on boundaries** on where, when, and how they should use their devices. You can set up a family agreement that the whole family can sign-up to help build up good digital habits in your home. This could screen-free zones in the house or which apps they should or shouldn't use on their devices.

3. For younger children, **make use of the free parental control tools** available on the devices they use to create a space where they can explore safely. This includes

setting home broadband filters to block inappropriate content or using apps like Screen Time on Apple or Google Family Link on Android phones to manage what they do on their devices

4. **Have age-appropriate conversations** about what they might see online so they feel confident to come to you for support if they see something that upsets them or makes them feel uncomfortable.

For age-specific advice to keep children safe online visit internetmatters.org/advice