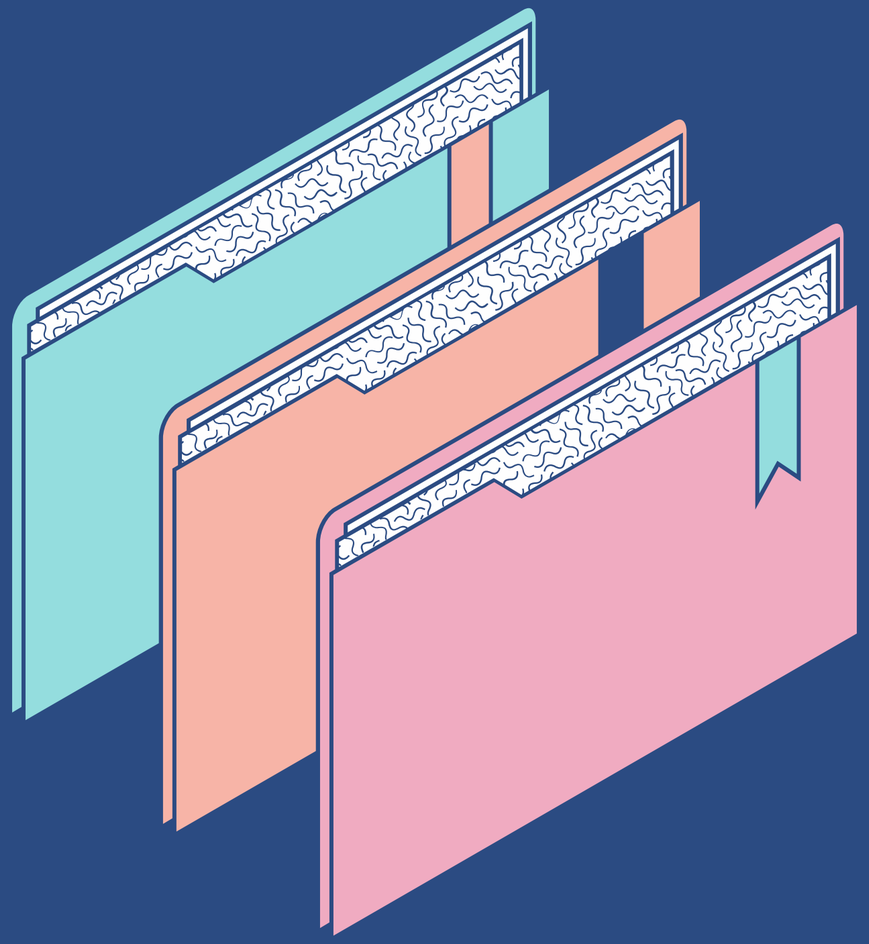
Milton Keynes age UK

DIGITAL INCLUSION

Staying Safe Online

A look at the importance of protecting yourself and your data

Online safety is crucial to protect personal information, prevent cyberbullying, and ensure a safe and positive online experience for everyone.



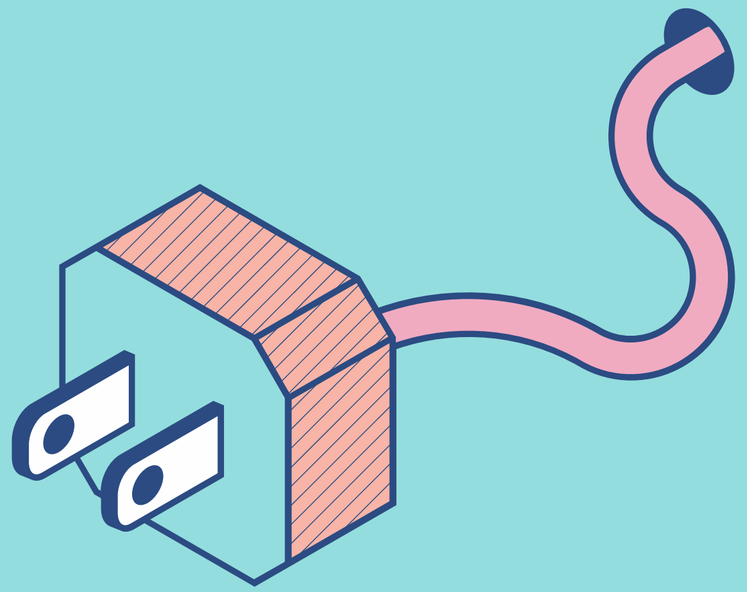
Agenda

KEY TOPICS

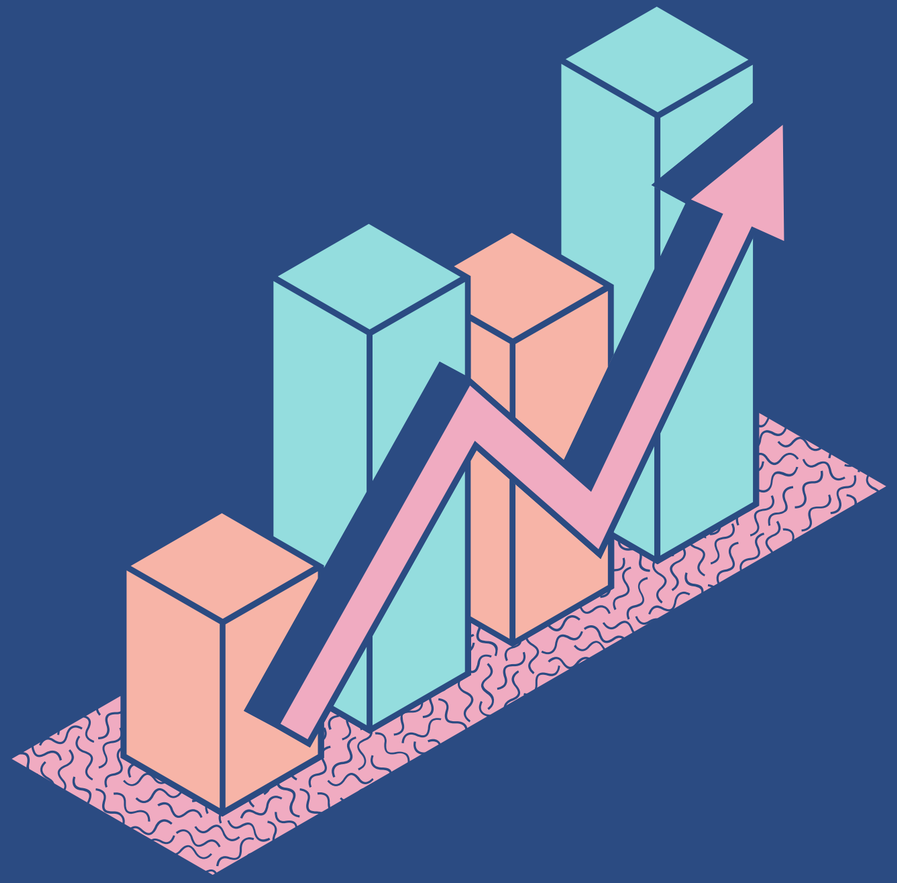
- Cyberbullying
- Passwords
- Social Media
- Online Privacy
- Phishing
- Mental Health

Being Safe in 2023

In today's digital age, the internet has become an integral part of our lives. However, with the vast opportunities that the internet offers, come risks and threats that can compromise our safety and security. In this presentation, we will explore some of the key issues surrounding online safety and provide practical tips and strategies to help you stay safe online.



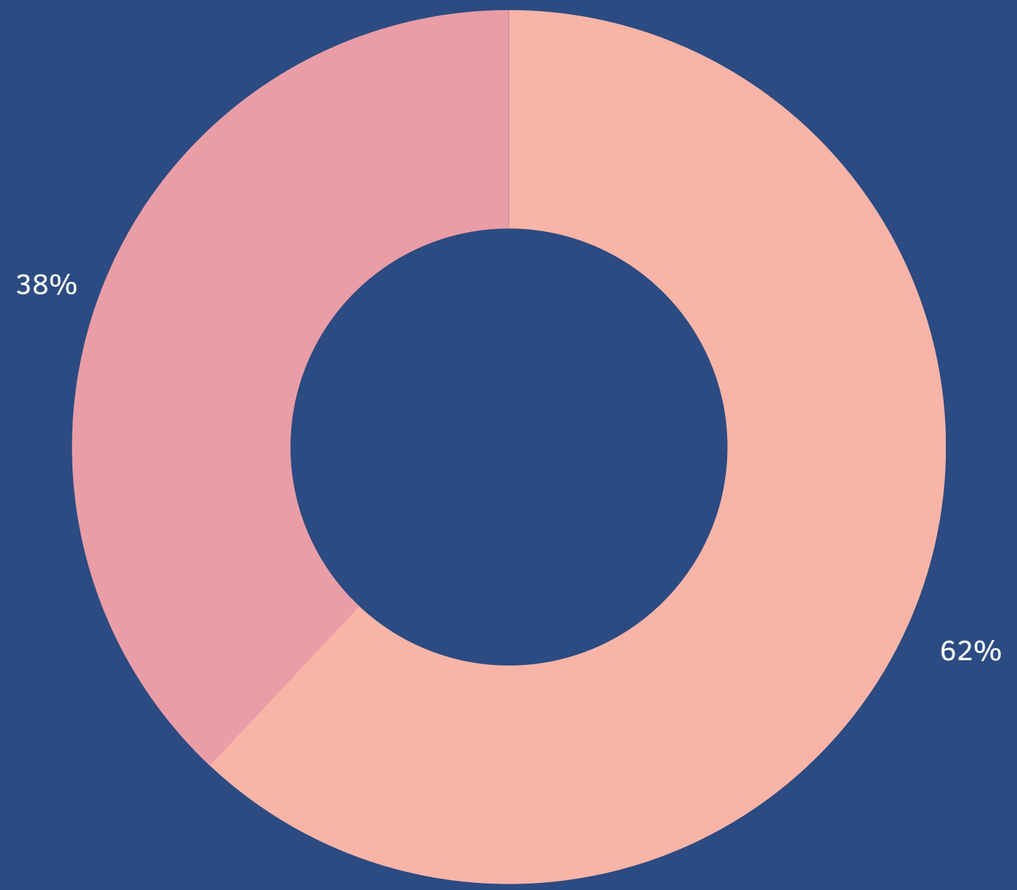
Game Time!



62% of adults have had harmful experiences online

ACCORDING TO THE UK GOVERNMENT

This is compared to 80% of children
who have been a victim of online harm.



Cyberbullying

CYBERBULLYING IS THE USE OF TECHNOLOGY TO HARASS, EMBARRASS, OR INTIMIDATE SOMEONE.

- **Examples**: Name-calling, spreading rumors, threats, and sharing embarrassing photos or videos.
- **Impacts**: Cyberbullying can have severe psychological and emotional impacts, including anxiety, depression, and in some cases, suicide.
- **Prevention**: Encourage victims to talk to someone they trust, avoid responding to the bully, and block or report the bully to the relevant platform.

How to be safe with passwords

1 STEP

Understand the importance of keeping safe.

A strong password is crucial to protect online accounts from hacking and unauthorized access.

2 STEP

Make a strong password.

A strong password should be at least 12 characters long, with a mix of upper and lower case letters, numbers, and symbols.

3 STEP

Manage your passwords effectively.

Never reuse passwords across different accounts, and keep a note of them in a safe place.

4 STEP

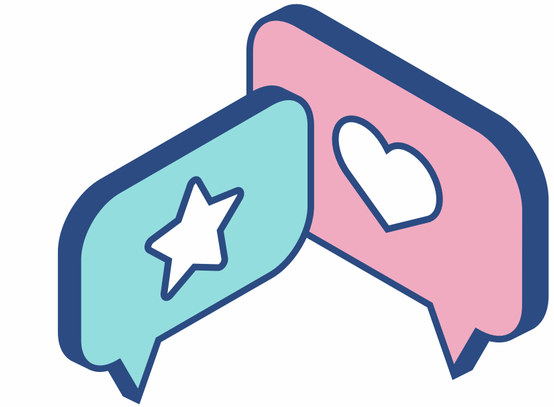
Consider two-factor authetication.

Enable two-factor authentication wherever possible to add an extra layer of security to online accounts.

5 STEP

Keep your passwords regularly updated.

Regularly update passwords and avoid writing them down or sharing them with others.



Social Media Safety

- **Privacy Settings**: Control who can see your posts, photos, and personal information.
- **Think Before You Post:** Consider the potential impact of your posts on your reputation and future opportunities. Avoid posting personal or sensitive information online.
- **Friend Requests**: Be cautious when accepting friend requests from people you don't know in real life. Scammers and cybercriminals often use fake profiles to target victims.
- **Cyberbullying:** Report and block any cyberbullies and avoid engaging in online arguments.
- **Phishing Scams**: Be wary of suspicious messages, links, and requests for personal information. Verify the authenticity of requests before providing any information.

Online Payments

HOW TO BE SAFE SHOPPING ON THE INTERNET

Ultimately, the decision to save your card details online should depend on your comfort level with the risks and your trust in the security measures in place by the company or website.

Use reputable websites and companies

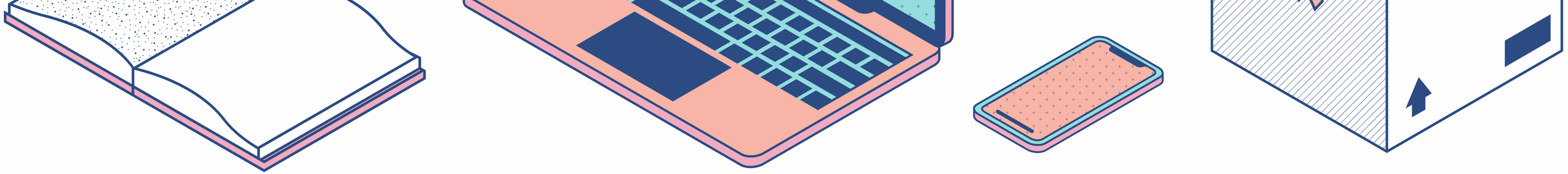
Reputable companies use encryption and security measures to protect your information.

Check your card transactions and statements

Catch any suspicious or fraudulent activity early on - you can get your money back!

Keep your online accounts safe and secure

Remember to regularly change your passwords and make sure they're strong and unique.



Secure Searching

- Search engines such as Google Chrome have built in security
- Use anti-virus protection to detect any bugs or harmful software - like McAffee
- Regularly update your devices to keep everything up-to-date and running smoothly
- Firewalls act as a barrier between your computer and the internet, and only allows safe and authorized traffic to enter and leave your computer.
- Secure websites have a lockbox in the search bar at the top of the screen
- You can report suspicious sites to the police

Phishing

BE AWARE ABOUT SHARING PERSONAL IMFORMATION

Phishing is a type of cyber attack where scammers try to trick you into revealing your personal information

This includes your login credentials, credit card details, or other sensitive information.

They usually involve an email or a message that appears to be from a legitimate source

The email or message may ask you to click on a link, open an attachment, or provide your personal information.

Scammers can access your sensitive data and use it for fraudulent activities.

Phishing attacks are becoming more sophisticated and difficult to detect. Some scammers may use social engineering techniques to gain your trust.

Phishing

HOW TO RECOGNISE
THEM AND STAY SAFE

Verify the source

Get in contact with the real company to confirm it's a legitimate request.

Look for mistakes

Look for spelling or grammar mistakes, check the sender's email address, and avoid opening attachments from unknown sources.

Use anti-phishing software or browser extensions

These can detect and block suspicious websites or emails.

What to do if you get scammed

THERE IS A WAY OUT!

- Stop all communication with the scammer and do not provide any more personal information.
- Take screenshots or save copies of any messages, emails, or web pages related to the scam.
- Contact your bank or credit card company immediately to report any unauthorized transactions or fraudulent charges.
- Change your passwords and enable two-factor authentication for all your online accounts.
- Report the scam to the relevant authorities.
- Consider getting help from a reputable identity theft or fraud recovery service. They can help you with the legal and financial aspects of the scam and assist you in recovering your losses.

Mental Health

- Technology can have positive and negative effects on our mental health.
- Cyberbullying, social media addiction, and exposure to harmful content can negatively affect our mental health.
- There are also positive resources that can positively affect our mental health.
- Online safety measures such as using strong passwords, being cautious of phishing scams, and limiting screen time can help mitigate these risks.

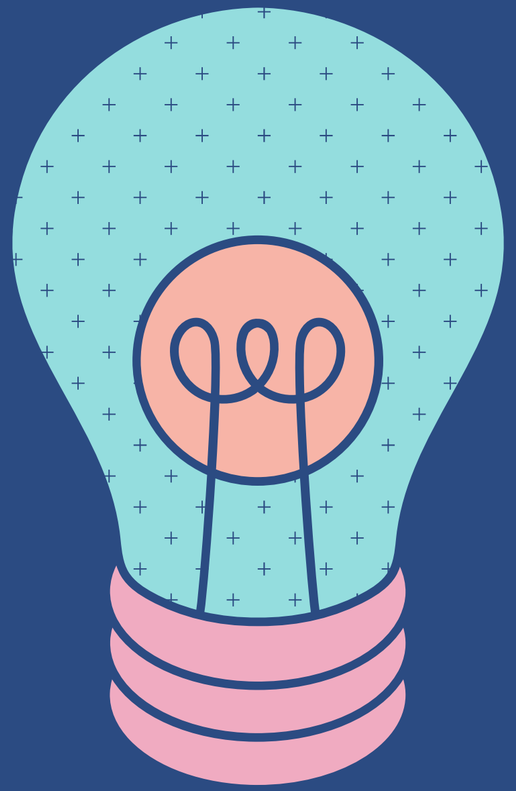
Useful Resources

LEARN MORE!

- Age UK resources
- Stay Safe Online Website
- Government Resources
- Password generators
- Two-factor authentication apps

"Online safety is not just about protecting devices, it's about protecting people."

JULIE MHYER



Do you have any questions?

This is your time to get any help you may need with your devices.