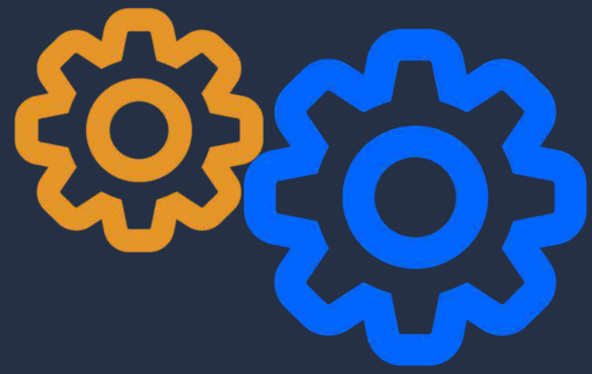
internet matters.org

How to create secure accounts online

Guidance on two-factor authentication (2FA), strong passwords and more

What's in this guide?



- Why do children need strong account security?
- Creating a strong password
- What is two-factor authentication (2FA)?
- Other cyber security risks to look for
- Software to keep your family cyber secure

Back to main menu

Why do children need strong account security?

Jump to...

Why do children need strong account security?

Children's vulnerability

Children are some of the most vulnerable users online. Creating secure accounts means others are less able to take advantage of them.

Georgie Price from Internet Matters' partners, ESET, says "Children are not always conscious of the risks associated with downloading files from unknown sources."

She adds, "Malicious links often exploit a child's curiosity and naivety; the phishing and ransomware attacks begin with a simple click."

Back to contents

Why do children need strong account security?

Teaching critical thinking

Thinking critically about information and people online is key to digital literacy. Secure accounts help children learn these skills that are still developing.

Psychologist and Internet Matters Ambassador, Dr. Linda Papadopoulos says, "[Children] are in an environment [online] where they're on their own for a lot of the time."

So, it's important to help them develop the skills they need by using tools that are available, such as using privacy and security features to create secure accounts.

Back to contents

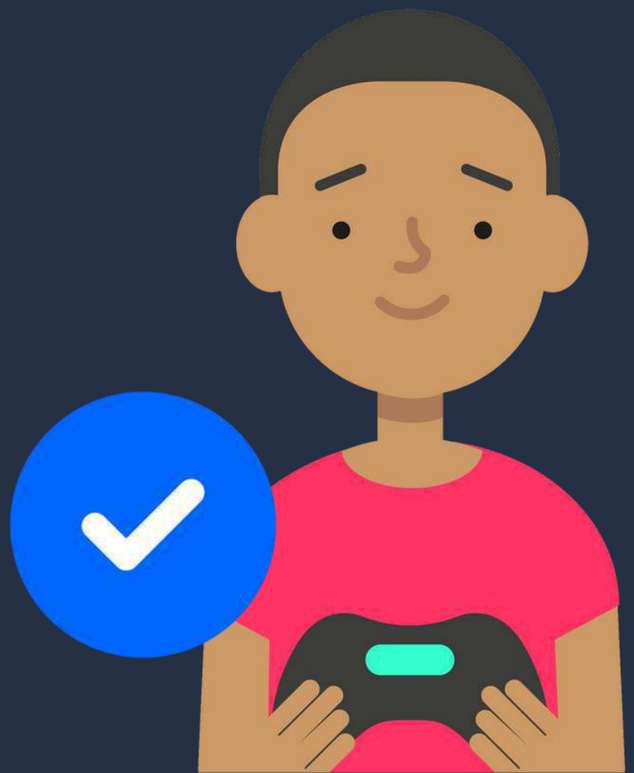
Why do children need strong account security?

Creating a safety net

Just like riding a bike, children need to be taught how to use their digital space and how to stay safe.

"When your child rides a bike, you don't just pop them onto a bike and go, 'there you go,'" says Dr. Linda. "You start off with a tricycle, then you have training wheels, then you take those training wheels off, but you hold on tight. And then, when they feel confident, you do let go. There is a sense of progression."

Setting up secure accounts provides children with a safety net to help them learn digital literacy skills safely.



Back to contents

More resources

Back to main menu

Learn more about children's development and online safety needs with the resources below.

[The Digital Resilience Toolkit]

[Online Critical Thinking Guide]

[Online safety advice by age]

[Set up safe checklist]

[Step-by-step parental controls guides]

NEXT SECTION

Back to main menu

Creating a strong password

Jump to...

What is a data breach?

Data breaches can happen to anyone, but children's vulnerability online make them more at risk.

According to the National Cyber Security Centre (NCSC), a data breach is when a cyber criminal gets access to information without permission. Criminals usually do this by using their technical skills to hack into computers or websites.

If a cyber criminal gains access to your child's details, advises the NCSC, "they can use it to create convincing phishing emails or scam text messages . . . to trick recipients into providing valuable information, such as their passwords."

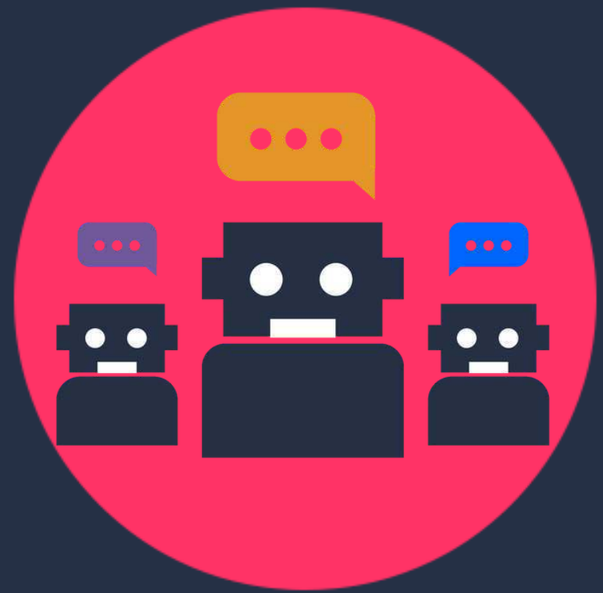
Back to contents

Creating a strong password

Using strong passwords to prevent data breaches

If your child's details are stolen in a data breach, criminals will try and access their accounts by trying the really obvious passwords that millions of people use.

"This is why it’s really important that you and your child’s online passwords are strong and secure," says the NCSC. "Weak passwords can be cracked in seconds. The longer and more unusual your password is, the harder it is for a cyber criminal to crack."



Back to contents

Tips for creating strong passwords

As your child starts to create online accounts, it's important they understand how to choose a strong password.

1. Avoid common passwords that can be easily guessed

"This might include a birthday, a favourite team or the name of a family member or pet. This kind of information may exist . . . online, which means they are easy to find out."

Back to contents

2. Use three random words

"Choose any three random words and put them together to create a single password. For example, ‘apple’, ‘nemo’ and ‘biro’ could become applenemobiro." These passwords are hard to guess.

3. Use a different password for every account

If one account is hacked, the cyber criminal will not be able to access any other accounts if the passwords are all different.

Write the different passwords somewhere safe and away from devices, use a password manager or save them in-browser to remember them.

Back to contents

Creating a strong password

More resources

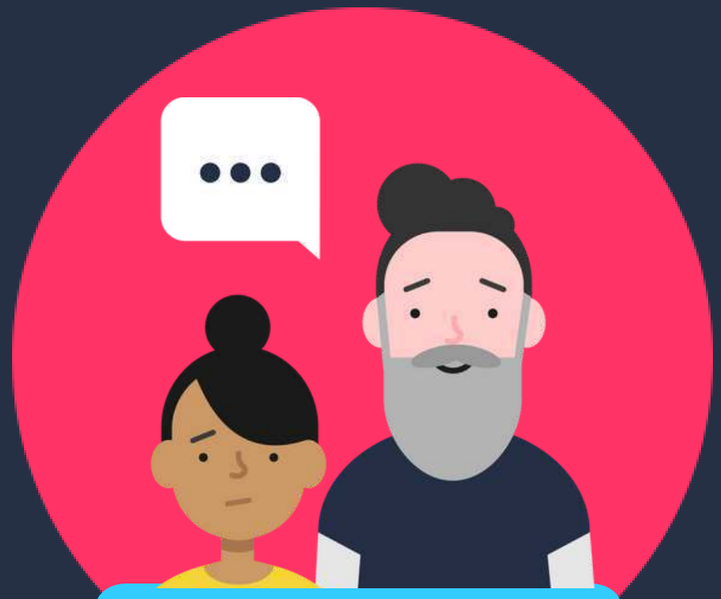
Back to main menu

Learn more about data breaches, strong passwords and cyber security with the resources below.

How a strong password protects from data breaches

What is cyber security?

Digital Matters:
Protecting Personal Information Online



NEXT SECTION

Back to main menu

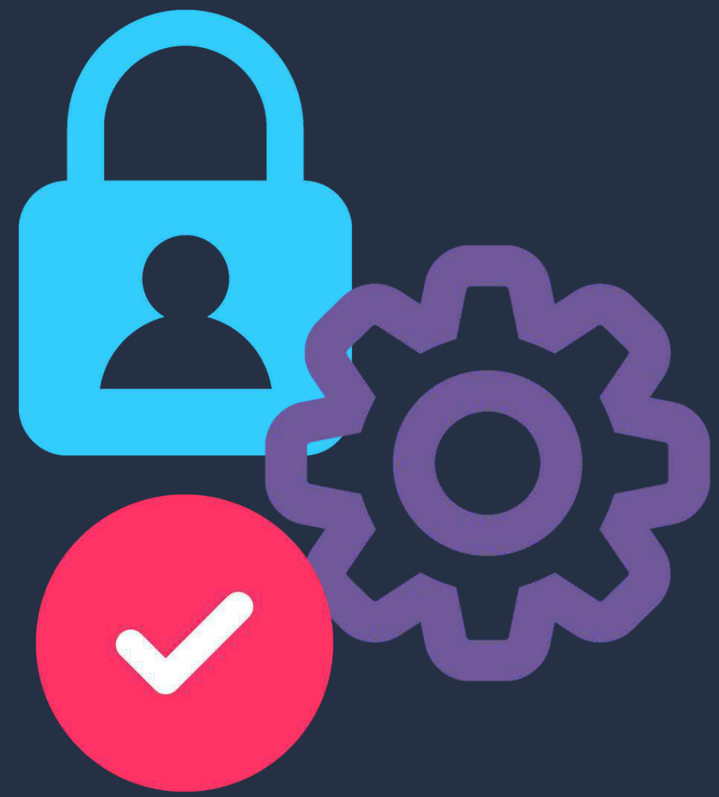
What is two-factor authentication (2FA)?

Jump to...

Should I use 2FA? →

How to set up 2FA →

More resources →



What is two-factor authentication (2FA)?

Should I use 2FA?

Two-factor authentication, also called two-step verification (2SV) or multi-factor authentication (MFA) helps create more secure online accounts.

Using 2FA means that users and cyber criminals cannot login to an account with just a username and password.

"[It] works by prompting you to provide something in addition to the password (such as an SMS code that’s sent to your or your child’s phone)," says the NCSC.

Some parental controls offer this feature to allow parents to confirm account access, adding additional security.

Back to contents

How to set up 2FA

According to the NCSC, "all social media platforms allow you to turn on 2-Step Verification (2SV)."

While 2FV is available across platforms, how you set this up will vary. However, you can usually find this setting with these steps:

1. Open the app and go to your **account settings**.

2. Find the setting labelled '**Privacy and Security**', '**Security**', '**Account Settings**' or similar.

3. Locate '**Two-Factor Authentication**' or '**Two-Step Verification**' or similar.

4. Follow **in-app instructions** to set it up. You may need a **separate device or email**, depending on the app.

Back to contents

More resources

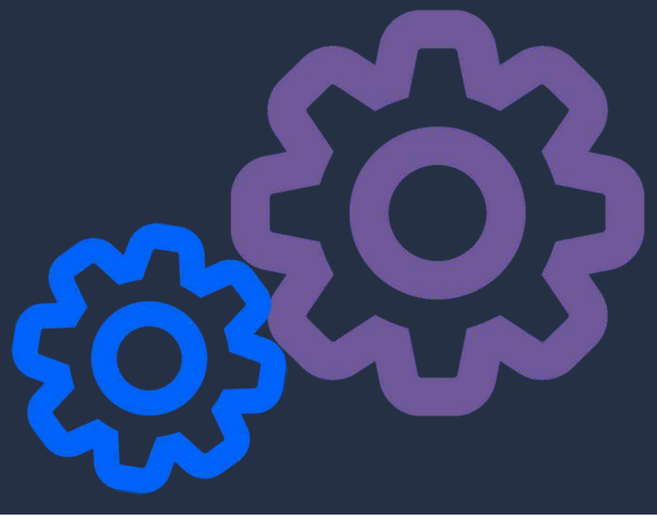
Back to main menu

Learn more about two-factor authentication (2FA) and additional account security with the resources below.

Step-by-step parental controls guides

How to tackle online scams: Expert advice on social media security

NCSC: Turn on 2-step verification (2SV)



NEXT SECTION

Back to main menu

Other cyber security risks to look out for

Stay informed on cyber security risks that could impact your family with the guides below.

[ESET's guide to phishing and ransomware]

[What is doxxing? How to keep children safe]

[Privacy and identity theft advice hub]

[Cyber security: Types of cyber attacks]

NEXT SECTION

Back to main menu

Software to keep your family cyber secure

Jump to...

Our partner, ESET →

Paid software →

Free software →

Software to keep your family cyber secure

Our partner, ESET

Security company and Internet Matters partner boasts highly rated antivirus software for home and devices.

ESET antivirus software offers:

- flexible plans to decide the number of devices you need and for how long
- data encryption
- password management
- privacy and banking protection
- protection against cyber attacks
- different options to test and trial the software.

GO TO ESET >

Back to contents

Software to keep your family cyber secure

Paid software

See below a few of the top paid software to support family security online.

Norton 360 Advanced

Families use it because: It provides a range of security features and provides a secure VPN service along with social media monitoring and identity theft support.

Cost: £39.99 for the first year

GO TO NORTON >

McAfee Total Protection

Families use it because: It provides families with a firewall, secure VPN, parental controls along with antiviral protection and great technical assistance from the McAfee team.

Cost: £49.99 for the first year

GO TO MCAFEE >

Back to contents

Software to keep your family cyber secure

Paid software

See below a few of the top paid software to support family security online.

Bitdefender Premium Security

Families use it because: It's an all-in-one software for enhanced cyber security. As such, it offers protection for your data and passwords as well as against spam, fraud and phishing.

Cost: £54.99

GO TO BITDEFENDER>

Back to contents

Software to keep your family cyber secure

Free software

See below a few of the top free software to support family security online.

Avast One Essential

Families use it because: It offers similar features to paid-for options such as malware protection and an optional VPN, as well as options to check for data breaches and compromised passwords.

GO TO AVAST >

AVG Antivirus Free

Families use it because: Just like paid options, it offers regular scans and protection against a variety of online threats. It is also specifically designed for personal and family use, which means it offers the right protection.

GO TO AVG >

Back to contents

Software to keep your family cyber secure

Free software

See below a few of the top free software to support family security online.

Microsoft Defender

Families use it because: It is automatically installed on PCs with Windows and offers great protection against malware and ransomware that could impact account and device security.

GO TO MICROSOFT >

RETURN TO START