Do you have a child starting at uni this Autumn?



Help them avoid a tough lesson by keeping safe online.





With coursework, tests, a hectic social life, visits to the laundrette, staying solvent and a host of distractions, there's a lot crammed into the life of a student.



So the last thing they may be thinking about is the possibility that they could fall victim to online harm.

Research shows that young people tend to take more risks and are therefore more vulnerable to fraud or abuse perpetrated on the internet. At best, this could result in inconvenience, embarrassment or losing a small amount of money. At worst, it could adversely affect their finances, reputation, wellbeing and even their whole future. including ending up with a criminal record. But you can help them enjoy a trouble-free online life.

Please share the tips on this page with your child ... it's one less thing to worry about.

Avoiding fraud

Fake texts, emails, DMs and calls claiming to be from the bank, student loan provider or HMRC are commonplace. Overseas students can be targeted by visa fraudsters too. Not thinking before they click – or oversharing – could cost your child their money, identity, or both.

Banking

Your child should follow their bank's security advice, including keeping their banking and other financial details private, and making money transfers safely via their bank's app. They should also get to know their Student Money Adviser.

Making payments

Payment by bank transfer to an unknown person or company for accommodation deposits, fees or other costs or purchases should be avoided where possible. If it's a fraud, there's very little chance of getting a refund from the bank.

Rentina

If you child has found accommodation they like, help them check it out in person and that the advertiser is authentic before any money changes hands. Ideally, deposits and other up-front payments should be paid by credit card for extra protection.

Posting

What goes online stays online, including things your child might regret sooner or later. 70%* of employers look at social media to screen candidates before hiring. Intimate images shared innocently can fall into the wrong hands. Location settings on phones and apps should be checked to help protect physical safety.

* Figures taken from a 2017 survey from CareerBuilders: https://www.careerbuilder.com/advice/social-media-survey-2017

Oversharing

Your child will need to prove their identity to open or access their bank account, sign up for a railcard, student discount or other essentials.

They should never reveal logins or other passwords and **not overshare** online, in texts or on the phone. This includes providing confidential information in return for freebies or to be entered into prize draws.

Being responsible

Reinforce that there's no place online for any kind of abuse, hate speech, forcing their views on others or criminal activity.

Using mobile devices and Wi-Fi

Phones, tablets and laptops should be protected at all times. If what your child is doing is confidential or financial, they should avoid using Wi-Fi hotspots as there's no guarantee they're secure. Warn your child about location services on apps too.

Gambling

For some students away from home, betting can become a bad habit. Remind your child how much money and time they could be wasting and the positive things they could do with it. Point out the fine line between gaming and gambling.

Dating

It's essential to use a reputable app and keep conversations on the app's messaging platform.

Not everyone is who they claim to be ... some even use online dating to commit fraud or endanger their date's physical safety when they meet up.

safety when they meet up. Tell them not to be afraid to block or say no.

No means no

Your child should never be put under pressure to do something they feel uncomfortable with, or put others under pressure. This includes sending or publishing

intimate pics, harmful pranking, extreme content, hacking others' social media accounts or any kind of radicalisation.

'Get rich quick' schemes

Students are favourite targets for illegal get rich quick schemes, like jobs with pay that's too good to be true or others using their bank accounts to 'process payments'. Money muling or laundering could result a criminal record, even if it's done unwittingly.

Keep coding legal

Students who are clever coders and extraordinary gamers are sometimes targeted by cybercriminals who need their skills for malware coding or hacking. Talk to your child about the consequences and discuss alternatives like a career in cybersecurity.





Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit www.getsafeonline.org



If you think you have been a victim of fraud, report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. If you are in Scotland, contact Police Scotland on 101.



www.getsafeonline.org



