Being at uni or college is about studying hard and enjoying the experience.

And, it's about taking more responsibility for yourself.

We're not talking total adulting. But there are definitely things you need to do to keep yourself, your finances and your devices free from harm online and offline, whether you're studying, out having fun or relaxing. Our experts have put together some top tips to start you off.

Look after your money
If you haven't already done so, you'll need to open an account, directly, with a respected bank. It's vital that you **keep your banking and other financial details private**. Most unis and colleges have a Student Money Adviser: talk to yours if you need advice on any other aspect of your finances.

Betting on a win?
For some people, **a bit of harmless betting can turn into a habit**. If you're tempted, think about how much money and time you could be throwing away and what else you could do with it. And sometimes, there's a fine line between gaming and gambling … don't cross it.

Payments
If you pay a person or company you don't know by **bank transfer** and it's a fraud, there's very little chance you'll get your money back, so try to avoid this wherever possible.

Dating apps
If you're dating online, use reputable apps and keep the conversation on the app. Remember that not everyone is who they say they are, and there's nothing more important than your personal safety whether you're dating or hooking up. **Don't be afraid to block or say no.**

Protect your reputation, and yourself
- **What goes online stays online** and that includes snaps and stories, as well as pics and posts, including those you might regret either immediately or in the future.
- Research shows **70%* of employers use social media to screen candidates before hiring**, so think about what you're posting and how it might affect you in the future when you start job hunting.
- Remember that online, not everyone is who they claim to be: consider this if you're talked into sharing intimate photos or videos. And for the same reason, remember that not every relationship lasts forever.

Be on the lookout for fraud
Fake texts, emails, calls and posts claiming to be from your bank, student loan provider or HMRC are rife for everybody … including students. If you're an overseas student, you could be targeted by visa fraudsters too. Not thinking before you click – or oversharing confidential information – could cost you your money, your identity, or both.

No means *no*
Never be put under pressure to do something you disagree or feel uncomfortable with, and **don't put others under pressure** either. We're talking sending or publishing intimate pics, harmful pranking, extreme content, hacking social media accounts or any kind of radicalisation.

Don't 'Unlock' your Smartphone
Also known as Jailbreaking or rooting, 'unlocking' your smart phone turns off software restrictions placed by the manufacturer, allowing you to download and install apps which aren't available through official app stores. This might seem like a good idea, but did you know you're also opening your phone up to dodgy apps and malicious software that can infect your phone and damage or delete the data you have on it?

Protect your ID, and don't overshare
The ability to provide ID is everything, and not just in a bar! Without it, you can't open or access a bank account, sign up for a railcard, student discount or other essentials.
- Never reveal logins or other passwords and **don't overshare** online, in texts or on the phone.
- Don't be tempted to provide confidential information on yourself or anyone else, in return for freebies.
- **Check your credit score** to make sure nobody has taken out credit or purchased anything in your name.

Accommodation
Found accommodation you like? **Check it out in person before parting with any money, and make sure who you're paying is authentic.** If you can, pay deposits and other up-front payments by credit card for extra protection.

Care with your tech and how you connect
Your phone, tablet and laptop are essential to your life, so **treat them like the precious possessions they are.** If what you're doing is confidential or financial, avoid using Wi-Fi hotspots: there's no guarantee they're secure. And turn off location services to keep your whereabouts to yourself.

Don't become a money mule
Get rich quick schemes, jobs advertised with pay that's too good to be true or trusting others with your bank account could result in a sentence criminal record. **Be wary if approached.**

Keep your coding legal
Heavyweight coders are sometimes targeted by cybercriminals who need their skills. If you get approached, think about the consequences to yourself and others.

Find comprehensive, easy-to-follow advice about online safety at www.getsafeonline.org

#safefresher

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 a number of government departments, 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

OFFICIAL PARTNERS

TESCO · HSBC · KASPERSKY · Royal Mail · Gumtree · Standard Life · TalkTalk · airbnb

Royal Bank of Scotland · NatWest · PayPal · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · first direct · creativevirtual The science of conversation

HM Government · CITY OF LONDON POLICE National Policing Lead For Fraud · NPCC National Police Chiefs' Council · NATIONAL TRADING STANDARDS eCrime Team · cifas Leaders in fraud prevention · VS VICTIM SUPPORT · EUROPOL EC3 European Cybercrime Centre

NCA National Crime Agency · National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk · METROPOLITAN POLICE · National Trading Standards Protecting Consumers Safeguarding Businesses · Ofcom · NEIGHBOURHOOD WATCH · TO STOP FRAUD · CYBER AWARE