GET SAFE ONLINE .org

CyberScotland
CYBERSCOTLAND PARTNERSHIP

www.getsafeonline.org

The young people in our families generally have a better hands-on knowledge of technology than we do. However, this confidence can result in them taking more risks online that could adversely affect their finances, reputation and potentially, their whole future.

That's why our experts have put together some tips to help you advise your child before they go to uni or college. Please take time to pass them on.

#safestudentonline

Your top student online safety tips

Safe banking

It's essential for your child to 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. Suggest they get to know their Student Money Adviser.

Protect their reputation, and themselves

What goes online stays online, including things your child might regret sooner or later. Remember that 70%* of employers look at social media to screen candidates before hiring. Intimate images shared innocently can fall into the wrong hands. Also check out the advice on the Young Scot website on how to remove unwanted images online.

Identity and 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. Suggest they check their credit score regularly to make sure nobody has taken out credit or purchased anything in their (or your) name.

Mobile devices and Wi-Fi

Phones, tablets and laptops **should be treated like the precious possessions they are**. 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.

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

Digital responsibility

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

Fraud

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

Buying online

You do have more consumer rights when buying online but it can increase your risks. **Always look for HTTPS** before entering your payment card details. A credit card can offer more consumer protection than a debit card.

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.

Consider having two bank accounts – one for online shopping and gaming and the other one for SAAS and wages payments in and paying bills out.

Online 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.

Online 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. **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 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.

Please see more tips overleaf. And find comprehensive, easy-to-follow advice about online safety at www.getsafeonline.org

Basic online safety tips

- Use strong passwords (you could start with three random words plus numbers and symbols), keep them to yourself and use separate ones for each online account.
- Use two-factor authentication as an additional security layer for online banking, shopping and other confidential activities.
- Check your digital footprint regularly for what others have posted about you or tagged you in.
- Learn how to spot and avoid commonplace scams.
- Protect mobile devices by using an access code, biometric face or finger print access and switching on the "find my phone" feature.
- Only download apps from the official "app stores" and make sure you apply your operating system updates as they are released.
- Regularly review your device's network, location and other settings.
- Check that payment pages are secure (https://) and that website addresses are legitimate.
- Avoid clicking on links in unexpected emails, texts and on social media, and email attachments. Forward actual or suspicious phishing emails to the NCSC suspicious reporting service via report@phishing.gov.uk
- Don't use public Wi-Fi hotspots for anything confidential, consider tethering your laptop with your mobile device to make your own virtual private network.

If you think you have been a victim of fraud contact Police Scotland on 101.

GET SAFE ONLINE .org

www.getsafeonline.org

CyberScotland

CYBERSCOTLAND PARTNERSHIP

GET SAFE ONLINE OFFICIAL PARTNERS

TESCO kaspersky Gumtree Standard Life first direct M&S BANK HSBC

Royal Bank of Scotland NatWest LLOYDS BANK HALIFAX BANK OF SCOTLAND creativevirtual The science of conversation™ ClearScore ROYAL AIR FORCE

ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk

NATIONAL TRADING STANDARDS eCrime Team Protecting Consumers Safeguarding Businesses

cifas Leaders in fraud prevention

VS VICTIM SUPPORT

NEIGHBOURHOOD WATCH

TAKE FIVE TO STOP FRAUD

EUROPOL EC3 European Cybercrime Centre

Ofcom