ARK Care

From the ARK Computer Repair workshop

Student safety pack

Free, plain-English guides to keep you safe online

Not sure about a message, email or call?

Call 01329 623 555

We'll tell you if it's a scam, free of charge. arkcare.uk

What's inside

The scams that target students, how to protect your laptop and your coursework, and what to do if something goes wrong. Free, quick to read, and written by real technicians.

1. Scams to watch out for
2. Student finance and HMRC scam messages
3. Renting safely: deposit and fake landlord scams
4. "Easy money" job offers and money mules
5. Back up your coursework before a deadline goes wrong
6. Getting your social media account back
7. Staying safe on public Wi-Fi
8. Passwords: the simple system that actually works
9. Two-factor authentication, explained properly
10. Need a hand?

Scams to watch out for

"Your student loan payment is on hold"

What it looks like: An email or text saying your Student Finance payment is suspended until you confirm your bank details through a link.

What to do: Don't click. Log in to your Student Finance account yourself. Forward scam texts to 7726 and emails to report@phishing.gov.uk.

Room or flat that seems too good to be true

What it looks like: A cheap room near campus, a landlord who can't show you round, and a request for a deposit before you've seen it.

What to do: Never pay before viewing. Use your university's accommodation service, and search the photos online to see if they've been copied.

"Easy money" through your bank account

What it looks like: A message on Instagram or Telegram offering cash to let money pass through your account.

What to do: Say no. That's money laundering, and it can close your bank account and affect you for years. Talk to your bank if you've already said yes.

"Can you send me the code I just sent you?"

What it looks like: A friend's account messages you asking for a login code, or to vote in a competition.

What to do: Never share a code. Their account has been hacked, and the code would let the scammer take over yours.

Student finance and HMRC scam messages

Scam messages spike around the start of term, when loan payments are due. They say your payment is on hold, your details need updating, or you're owed a tax refund.

The goal is your Student Finance login and your bank details, which can then be used to take your money or redirect your loan.

Signs it's fake

- A link asking you to "confirm" or "update" your bank details
- A deadline, such as "within 24 hours or your payment will be cancelled"
- A tax refund offer — students rarely have one due, and HMRC doesn't text links for them
- A sender address or link that isn't on gov.uk

How to check

Don't use the link. Open the Student Finance or HMRC website or app yourself, and log in there. If there's really a problem, it will show in your account.

If you entered your details

- Change your Student Finance password straight away, and any account that used the same password
- Call your bank on 159 if you gave card or bank details
- Contact Student Finance using the number on their website
- Forward scam texts to 7726 and scam emails to report@phishing.gov.uk

Renting safely: deposit and fake landlord scams

Student housing is competitive, and scammers use that pressure. They copy photos of real properties, advertise them cheaply, and ask for a deposit before you can view.

Warning signs

- The rent is noticeably cheaper than similar places nearby
- The "landlord" is abroad and can't show you round
- You're asked to pay a holding deposit before viewing
- Payment by bank transfer to a personal account, or in cryptocurrency
- Pressure that "lots of other students are interested"

Safer ways to rent

View in person, or ask a friend to. Use your university's accommodation service or a letting agent you can check. In England, a deposit should be protected in a government-approved scheme, and you should be told which one.

Search the property photos online. If the same pictures appear in other adverts, walk away.

If you've already paid

Call your bank straight away on 159, report it to Action Fraud on 0300 123 2040, and tell your university's accommodation office.

"Easy money" job offers and money mules

A message on Instagram, Telegram or a job site offers easy money: let some cash go through your bank account, keep a cut, and send the rest on.

This is money laundering. The person whose account is used is called a money mule, and they can lose their bank account, find it very hard to get credit, and face prosecution.

How the offers look

- "Work from home, no experience needed, earn hundreds a week"
- A "company" that wants your bank details before any interview
- Requests to receive money and transfer it on, or buy gift cards or crypto
- Paid "tasks" like liking videos, which later ask you to pay in first

What to do

Never let anyone else use your bank account, however small the amount. Genuine employers pay you a wage; they don't send money for you to pass on.

If you've already said yes, stop and talk to your bank now. Being honest early makes a real difference.

Back up your coursework before a deadline goes wrong

Laptops get dropped, spilled on, stolen or simply stop working, and it tends to happen at the worst possible moment. Extensions for lost work are not guaranteed.

The fix is easy: keep your work in more than one place, automatically.

The simple rule

Keep at least two copies of anything that matters, and one of them not on your laptop.

- Save coursework in the OneDrive or Google Drive account your university gives you
- Check that the files sync — look for the tick or cloud icon
- Keep a second copy somewhere else, such as a USB stick or a backup service
- Email yourself the final version before you submit, as a last resort

Sync is not quite backup

If you delete a file or it gets corrupted, cloud sync can copy that mistake everywhere. A proper backup keeps older versions, so you can go back to yesterday's copy.

If your laptop dies

Don't keep switching it on and off. If the drive is failing, that can make recovery harder. Stop and get it looked at.

Getting your social media account back

Account takeovers usually start with a message from a friend's hacked account: "Can you send me the code I just sent you?" or a link to vote in a competition. Once in, the scammer uses your account to trick your friends.

Act fast

- Check your email for a message from the platform saying your email or password was changed — it often has a "secure your account" link
- Use the app's official "hacked account" help page, not someone offering to recover it for a fee
- Change the password on your email account too, in case that was the way in
- Warn friends from another account not to reply to messages from you

Stop it happening again

- Turn on two-factor authentication, ideally with an authenticator app
- Never share a login code, even with a friend
- Use a different password for every account; a password manager helps
- Be wary of "vote for me" and "is this you in this video?" links

Beware recovery scams

People who post about being hacked are often contacted by "hackers" offering to get the account back for a fee. They can't, and they'll take your money.

Staying safe on public Wi-Fi

Public Wi-Fi used to be genuinely dangerous: anyone on the network could read what you were doing. Almost every website is encrypted now, so the old horror stories are largely out of date.

Some real risks remain, though, and they're not the ones people worry about.

What's still worth worrying about

The threats that survive are about who you're connecting to, not what passes over the air.

- Fake hotspots named to look official — "Hotel Guest WiFi Free" sitting next to the real one
- Sign-in pages that ask for far more than they need, or ask you to install something
- Certificate or security warnings in the browser, which you should never click past on a public network
- File sharing left switched on, exposing folders to everyone else on the network
- Someone simply reading your screen over your shoulder

Simple habits that cover most of it

None of this requires extra software.

- Ask staff for the exact network name rather than guessing from the list
- Turn off automatic joining of open networks, so your phone doesn't reconnect to a fake one later
- Set the network as Public on Windows, which switches off sharing
- Use your phone's own mobile hotspot for anything sensitive — it's usually faster anyway
- Keep the device patched, and keep antivirus running

Does a VPN help?

It genuinely does two things: it stops the network operator and anyone else on it seeing which sites you visit, and it protects you on badly configured or hostile networks. On a hotel, airport or conference network that's worth having.

What it doesn't do is make you anonymous or protect you from phishing, malware or a weak password. Treat it as one sensible layer rather than a shield. If you use one, pay for a reputable service — free VPNs make their money by selling the very browsing data you installed them to protect.

For people working away from the office

If work data travels with you, a VPN stops being optional. So does full-disk encryption (BitLocker on Windows, FileVault on a Mac), because the realistic loss is a laptop left on a train rather than anything clever happening over Wi-Fi.

Make sure remote access to the office goes through a VPN or a properly secured gateway with two-factor authentication — exposed remote desktop is still one of the most common ways businesses are breached.

Passwords: the simple system that actually works

Most accounts aren't broken into by guessing. They're opened with a password that was already stolen from somewhere else entirely — a shop, a forum, an old service that leaked years ago.

So the advice that matters isn't "make it complicated". It's "never use the same one twice".

Why reuse is the whole problem

When a company is breached, the stolen email-and-password pairs are sold in bulk. Automated tools then try those pairs on hundreds of other sites — email, shopping, banking. If you reused the password, they're in, and no amount of capital letters or exclamation marks helps.

You can check whether your own address has appeared in a known breach at haveibeenpwned.com. Most people are on at least one list, which is normal — it only matters if the password is still in use somewhere.

What a good password looks like now

The old rules produced passwords that were hard for people to remember and easy for computers to guess. Length beats complexity.

- Three or four unrelated words strung together, for example purple-harbour-kettle-92
- At least 14 characters where the site allows it
- Nothing drawn from your life: no names, pets, birthdays, street or football team
- No pattern you repeat across sites, like the site name plus your usual password
- Change a password when there's a reason to — not on a routine every 90 days

The three passwords worth memorising

You only need to hold a few in your head. Make these three long, unique and unwritten:

- Your email password — it's the master key, because every other account resets through it
- Your password manager's master password
- Your computer or phone unlock code

How a password manager actually works

It's an encrypted vault. You remember one strong password; it remembers everything else, generates new ones and fills them in for you. Bitwarden and 1Password are both sound choices, and the ones built into Apple, Google and Microsoft accounts are fine too if you live inside one of those.

The common worry — "isn't it dangerous to keep them all in one place?" — is understandable but backwards. The realistic risk isn't the vault being cracked; it's you reusing one password across 40 sites because remembering 40 is impossible.

If you'd rather use paper

A notebook is far better than reusing one password everywhere. Burglars are not after your passwords; automated credential stuffing is. Keep the book somewhere sensible, don't write the website next to each one in obvious terms, and never keep it in a file called passwords on the computer itself.

Two-factor authentication, explained properly

Two-factor authentication — 2FA, MFA, two-step verification — all mean the same thing: proving who you are with something more than a password.

It is the single most effective thing you can do for your online safety, and on the accounts that matter it takes about two minutes to switch on.

Why it works

A stolen password becomes useless on its own. The attacker has half of what they need, and the other half is sitting in your pocket. That's why almost every serious attack now tries to get around 2FA rather than through it.

The types, best first

They are not all equal, though any of them beats nothing.

- Security key or passkey — a physical key or your phone's fingerprint/face unlock. Phishing-proof, because it will only work on the real website
- Authenticator app — a six-digit code that changes every 30 seconds. Free, and works without signal
- Push approval — a "was this you?" prompt. Convenient, but never approve one you didn't trigger
- Text message code — the weakest, because numbers can be hijacked, but still far better than a password alone

Where to turn it on first

Start with the accounts that unlock everything else, then work outwards.

- Email — first, always; it's how every other account is reset
- Online banking and payment accounts
- Your Microsoft or Apple account
- Anywhere a card is stored: Amazon, PayPal, the supermarket
- Social media, so nobody can impersonate you to your friends
- For a business: remote access, accounting software and the payroll system

Set up recovery before you need it

This is the step people skip, and it's the one that causes the lockouts.

- Save the backup or recovery codes each service gives you — print them or store them in your password manager
- Add a second method, such as a partner's phone number or a second authenticator
- If you use an authenticator app, pick one that backs up to your account, so a new phone restores everything
- Don't store the codes only on the same phone that holds the app

Never approve a prompt you didn't ask for

If a code arrives or your phone asks you to approve a sign-in and you weren't signing in, somebody has your password. Don't approve it, and don't read the code to anyone who rings about it — that phone call is part of the attack.

Change that password straight away, then check the account's list of signed-in devices and remove anything you don't recognise.

Need a hand?

Is this a scam? Call us free

Ring **01329 623 555** and one of our technicians will tell you whether a message, email or call is genuine. There's no charge.

Keep your laptop protected all year

ARK Care plans include managed antivirus, updates checked and remote help when something breaks. We support you remotely wherever you study. If the laptop needs repairing, post it to our workshop and we'll courier it back. No long-term commitment, so you can cancel over summer.

See the plans at **arkcare.uk/products**.

Repairs from anywhere in the UK

If your computer needs our workshop, you can post it to us. We can help you book a courier, and we return it to you by courier. Postage is paid by the customer.

Useful UK numbers: call 159 to reach your bank safely · forward scam texts to 7726 · email scams to report@phishing.gov.uk · Action Fraud 0300 123 2040.