

SOUNDTRACK TO LIFE

Beware of the Scammers

Spot the signs. Pause. Check. Stay in control.

Ryan Powell
Ervin Miltenis
Stela Simeonova

Luton Borough Council

Today's playlist



01 **Cyber fraud** — What it is and why it works

02 **Five scam tactics** — Phishing, QR codes, deepfakes, passwords and impersonation

03 **Spot the scam** — Work through five realistic examples

04 **Public Wi-Fi** — How fake networks and fake login pages work

05 **Routes into cyber** — Real careers, different starting points



Fraud is designed to feel normal

4.5 million

estimated fraud incidents in England and Wales, year ending June 2026

Pause beats panic

Scammers do not need to “hack” you if they can persuade you to act.

Urgency

“Do it now”
“Your account will close”

Trust

A familiar brand, friend, bank or employer

Reward

A refund, prize, job, ticket or investment



How a scam works

1	2	3	4	5
Hook	**Pressure**	**Action**	**Capture**	**Repeat**
A message, call, advert or QR code	Urgency, fear, curiosity or reward	Click, scan, pay, share or install	Money, passwords or personal details	More contact, recovery scam or account takeover

Break the chain anywhere



Five scam tactics to recognise

Phishing

Fake emails, texts, DMs or calls

QR scams

A code hides the destination until you scan

Deepfakes

AI-made voice, video or images imitate someone

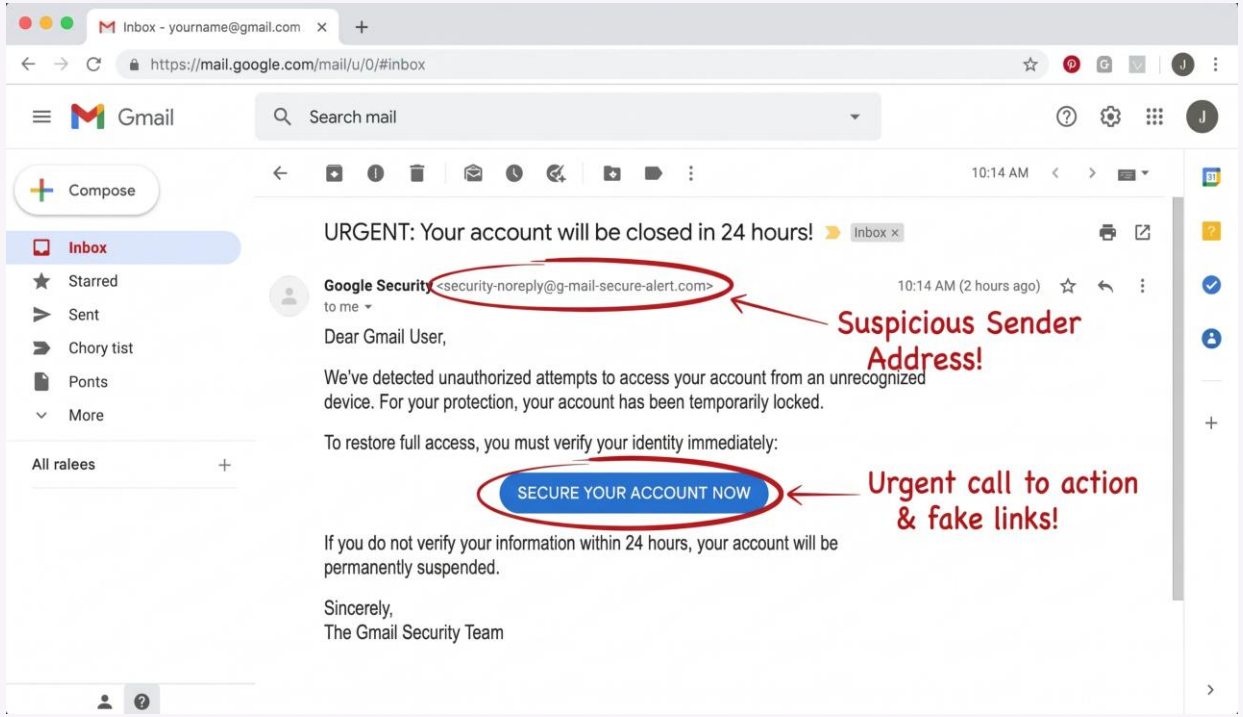
Password attacks

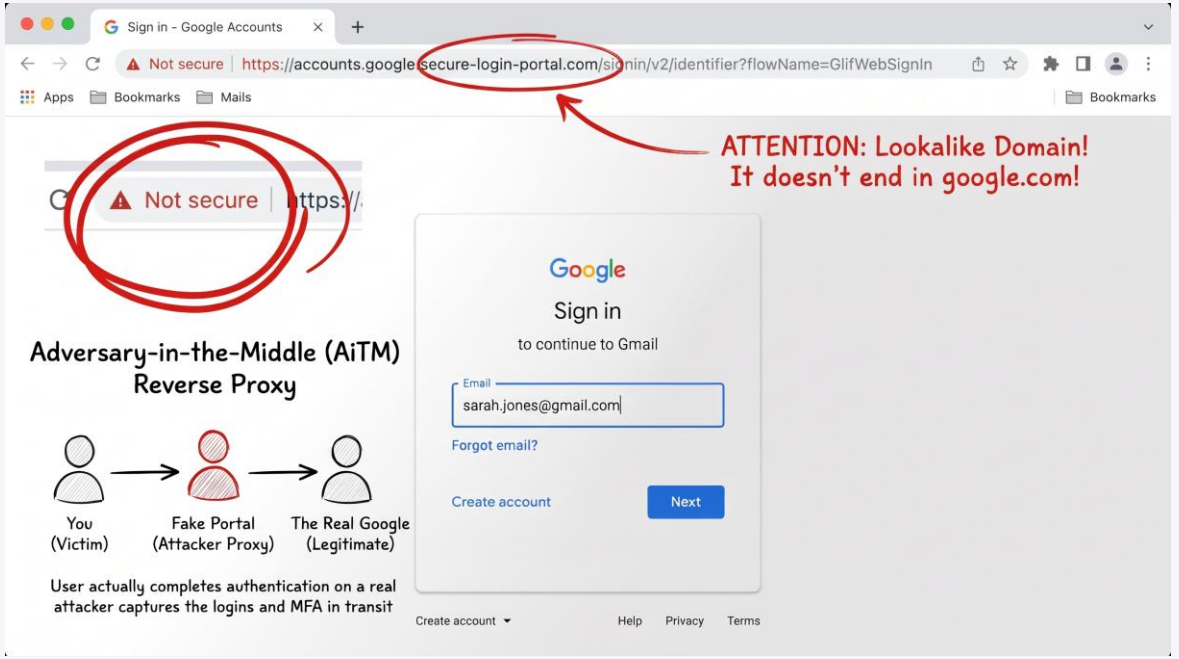
Stolen or reused passwords unlock more than one account

Impersonation

Someone pretends to be a bank, employer, police, friend or family

Phishing

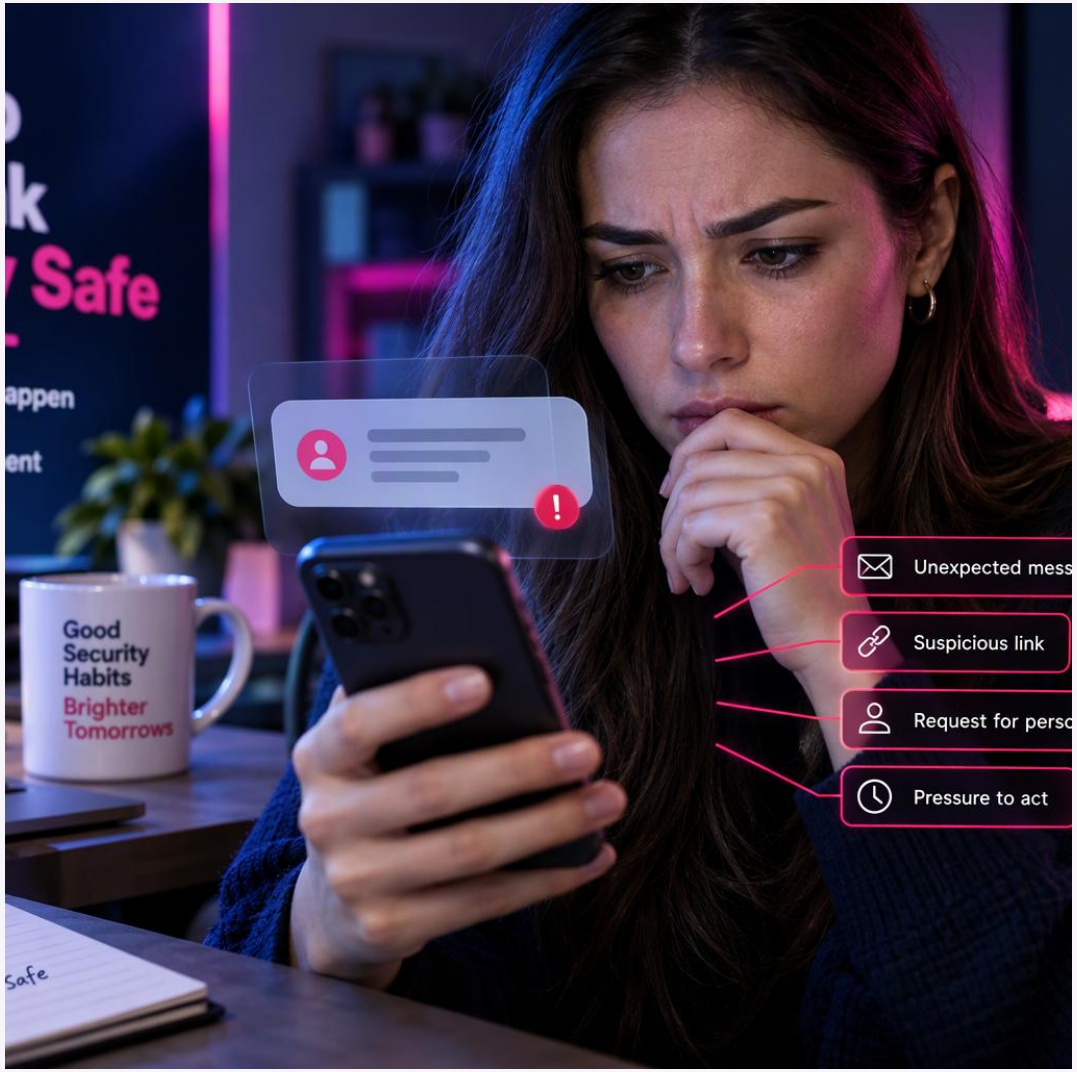

Inbox - yourname@gmail.com
https://mail.google.com/mail/u/0/#inbox
Gmail
Search mail
Compose
Inbox
Starred
Sent
Chory tist
Ponts
More
All ralees
10:14 AM
URGENT: Your account will be closed in 24 hours!
Inbox ×
Google Security <security-noreply@g-mail-secure-alert.com>
10:14 AM (2 hours ago)
to me
Dear Gmail User,
We've detected unauthorized attempts to access your account from an unrecognized device. For your protection, your account has been temporarily locked.
To restore full access, you must verify your identity immediately:
SECURE YOUR ACCOUNT NOW
If you do not verify your information within 24 hours, your account will be permanently suspended.
Sincerely,
The Gmail Security Team
Suspicious Sender Address!
Urgent call to action & fake links!


Sign in - Google Accounts
Not secure
https://accounts.google.secure-login-portal.com/signin/v2/identifier?flowName=GlifWebSignIn
Apps
Bookmarks
Mails
Bookmarks
ATTENTION: Lookalike Domain!
It doesn't end in google.com!
Not secure
https://
Adversary-in-the-Middle (AiTM)
Reverse Proxy
You (Victim)
Fake Portal (Attacker Proxy)
The Real Google (Legitimate)
User actually completes authentication on a real attacker captures the logins and MFA in transit
Google
Sign in
to continue to Gmail
Email
sarah.jones@gmail.com
Forgot email?
Create account
Next
Create account
Help
Privacy
Terms

Look for the pattern, not one typo

- Unexpected contact or a change to normal process
- Pressure to act quickly, keep it secret or avoid checking
- A link, QR code or attachment you were not expecting
- A request for passwords, one-time codes, card details or remote access
- Payment details changed at the last minute

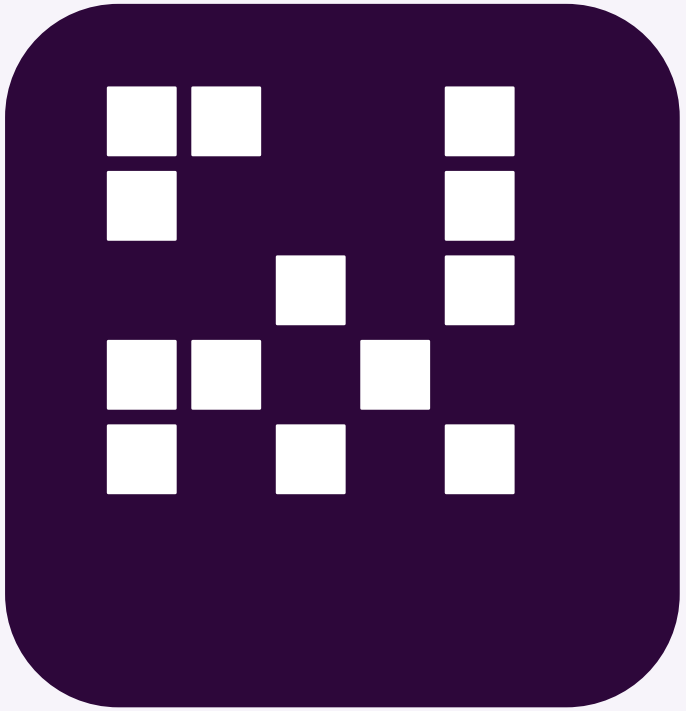
Best move: stop and verify through a trusted route you find yourself.



QR Survey



QR codes hide the link

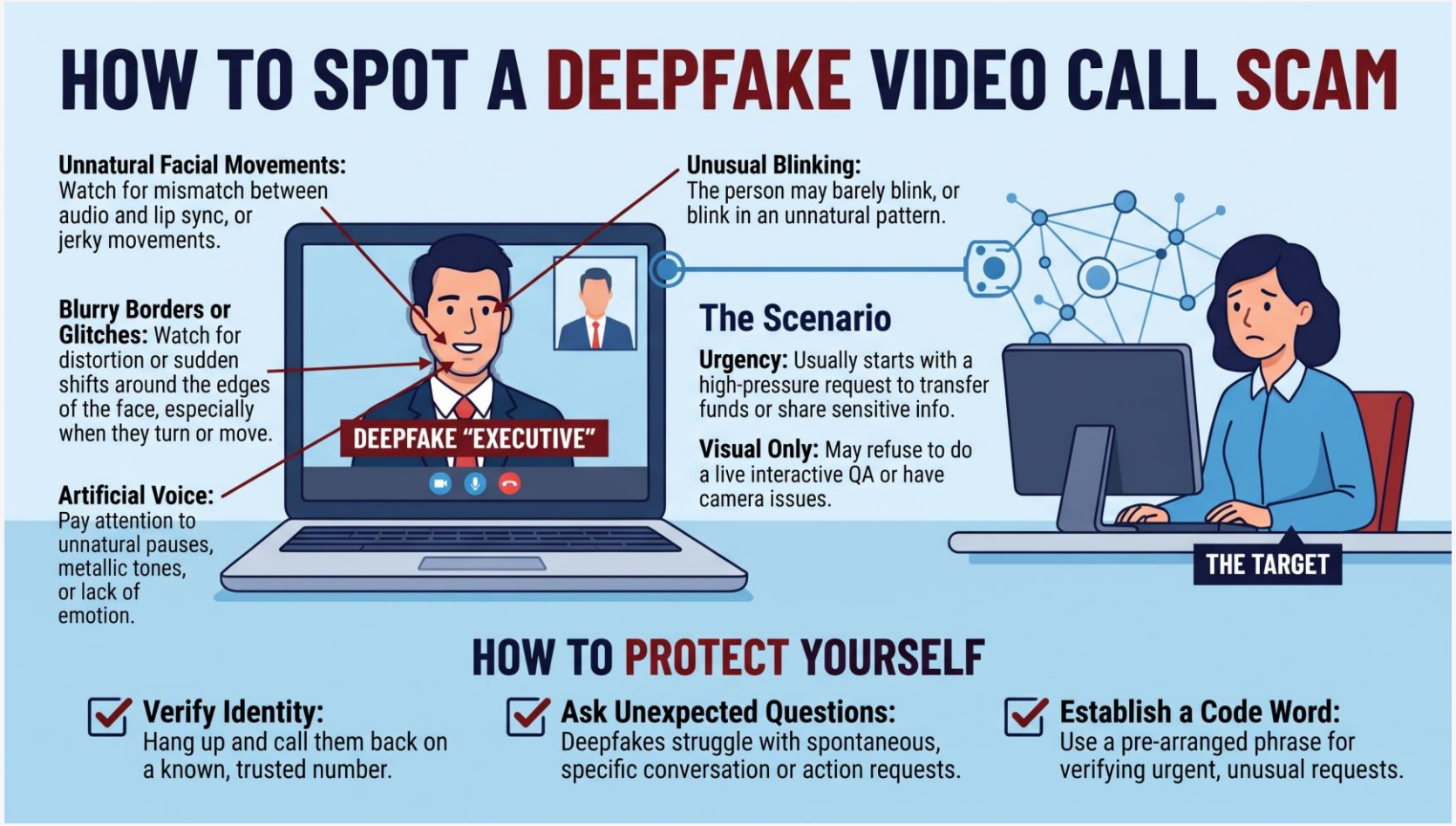


Before you scan

- Check whether a sticker covers the original code
- Use your phone camera, not a random QR app
- Preview the web address before opening
- Do not enter more information than makes sense
- For payments, open the official app or website yourself

A QR code is just a hidden link. Treat it like one.

Deepfakes: trust the process, not the voice





Deepfakes: trust the process, not the voice

Unexpected

A familiar voice or face contacts you from a new number or account

Urgent

They need money, a code or secrecy immediately

Unverifiable

They avoid a normal call-back or shared question

Your verification routine

- End the call or stop replying
- Contact the person using a saved number
- Ask a question only they should know
- Tell someone you trust before paying

"Sounding real" is not proof.

A separate check is proof.



Passwords: protect the keys to your life

Use unique passwords

A different password for email, banking and social accounts stops one breach spreading.

Make them long

Three random words are easier to remember and harder to guess.

Turn on 2-factor Authentication

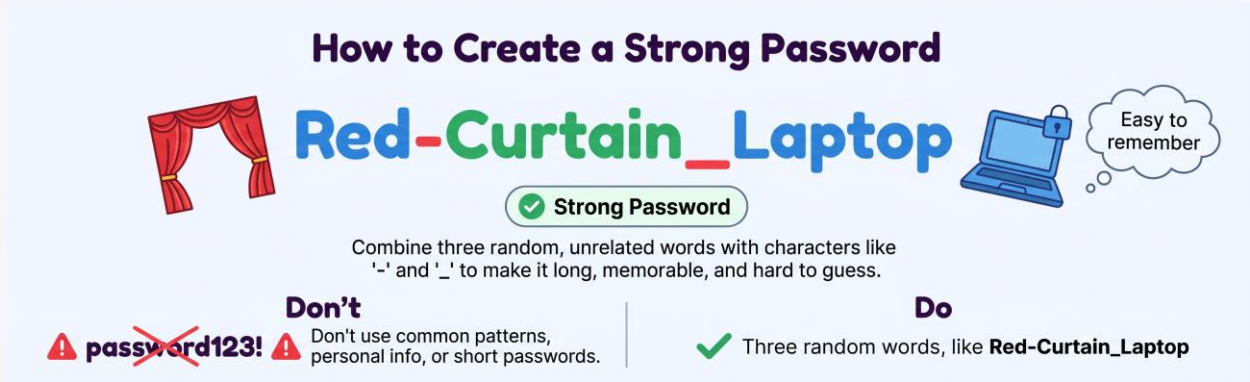
An authenticator app or passkey adds another barrier.

Protect your email first

Email resets other accounts, so it deserves your strongest protection.

Never share a one-time code with anyone who contacted you.

Passwords: protect the keys to your life







Spot the scam

You will see five messages. Decide:

1. Scam, suspicious or likely genuine?
2. What clues influenced you?
3. What would you do next?

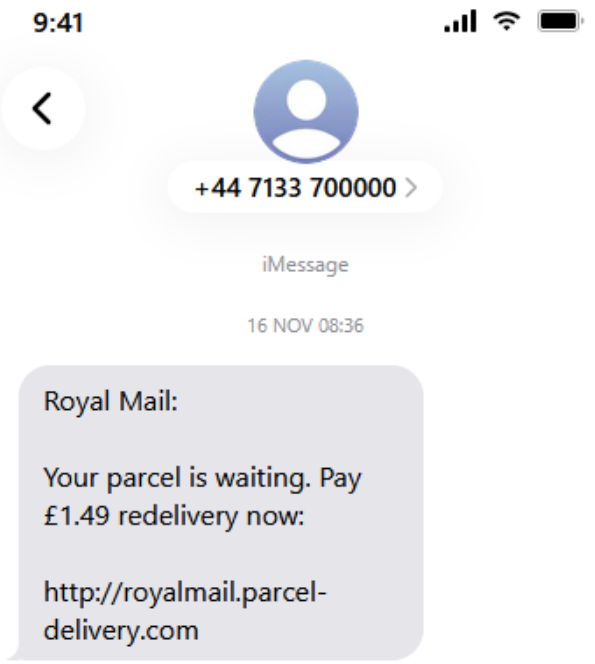
Rule

Do not click, scan, call or reply while deciding.

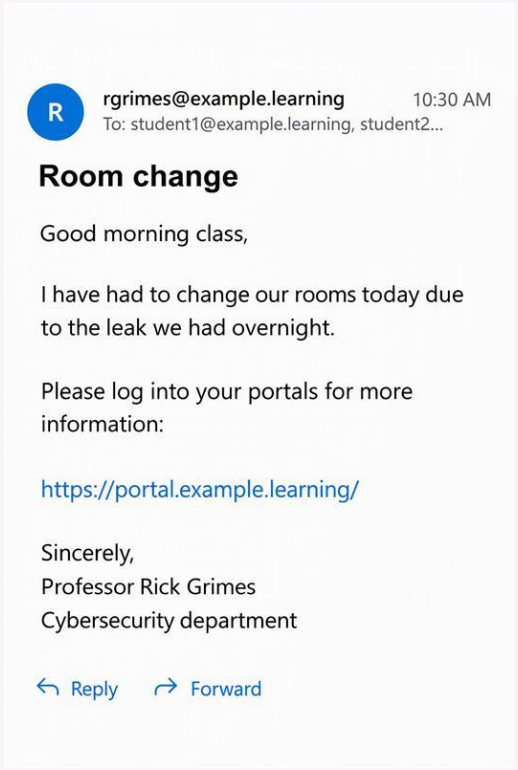
2 minutes, then we compare answers

Messages 1–3

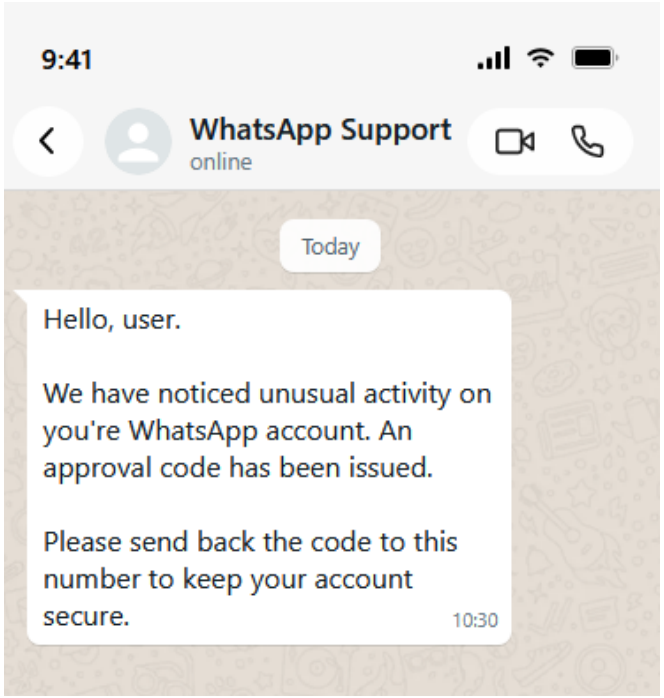
1 Text message



2 Email



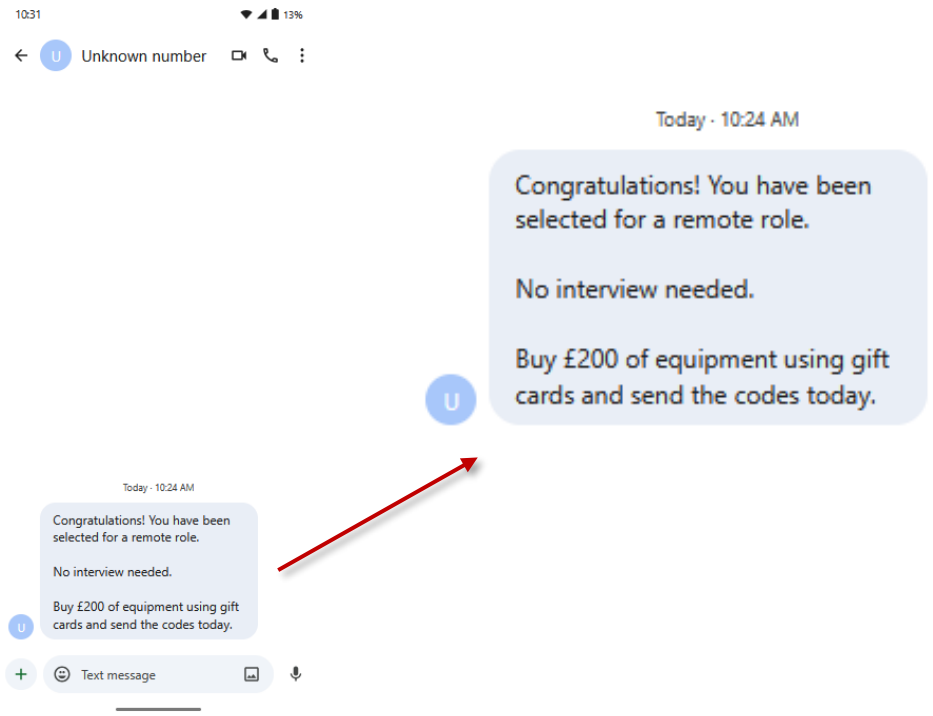
3 Support DM



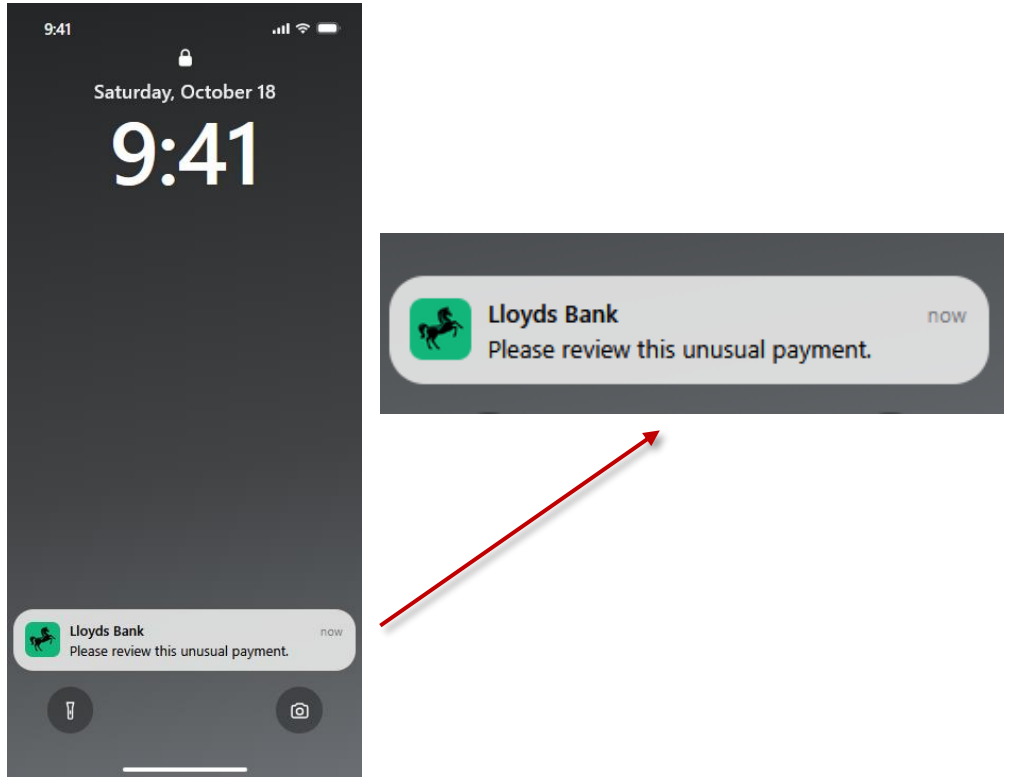
What would you check before acting?

Messages 4–5

4 Job offer



5 Bank notification



Which action keeps you in control?



The answers

1	SCAM	Lookalike domain, small fee, urgency
2	CHECK	Plausible, but verify in the student portal
3	SCAM	Requests a code and creates urgency
4	SCAM	No interview, gift cards, pressure
5	SAFER	Used the official app independently

The safest response usually moves away from the message.



If something feels wrong

STOP

Do not click, pay, reply or share a code

CHECK

Use the official app, website or saved number

TELL

Speak to someone you trust; contact your bank fast if money moved

REPORT

Report Fraud or forward suspicious texts to 7726

Being scammed is not your fault. Acting quickly can reduce the harm.

Public Wi-Fi: Convenient, but Can You Trust It?



- Public Wi-Fi is everywhere: cafés, airports, hotels and trains.
- Attackers can create convincing fake hotspots.
- Users may connect without realising they are using an attacker-controlled network.



The coffee-shop scenario: two names, one decision

YOU SEE

Wi-Fi

Starbucks WiFi

Could be genuine

Ask staff to confirm the exact network name.

Wi-Fi

Starbucks_Free_WiFi

Could be fake

A scammer can choose any believable name.

Why this works

- Wi-Fi names are labels, not proof of ownership.
- Phones may suggest or automatically rejoin familiar network names.
- A stronger signal can look more convincing than the genuine hotspot.

Stop. Ask staff. Connect only to the verified network.



How a fake hotspot attack unfolds

1. **Set up** — Attacker enables a Wi-Fi-capable laptop, phone, router or small access point.
2. **Imitate** — The hotspot uses a familiar name such as Starbucks_Free_WiFi.
3. **Attract** — The victim sees a strong, open network and connects.
4. **Prompt** — A captive portal asks for an email, password, code or card details.
5. **Pass through** — Internet access may continue so the victim suspects nothing.

The attacker does not need to “break” the real Starbucks Wi-Fi. The victim connects to the wrong network.



What the attacker is actually trying to capture

Credentials

Username, password, recovery answers or a one-time code entered into a fake portal.

Personal data

Email address, phone number, date of birth or card details used for later scams.

Insecure traffic

Data from old or badly configured apps that do not protect the connection correctly.

Session access

In limited cases, authentication tokens may be abused if another weakness is present.

Important: modern HTTPS normally prevents someone on the same Wi-Fi from simply reading every password.

The more realistic risk is a convincing fake page that persuades the victim to enter the information.



Six warning signs to disconnect

Unexpected login	The Wi-Fi asks for Microsoft 365, Google, banking or social-media credentials.
Lookalike name	The network name contains extra words, underscores or small spelling changes.
Security warning	The browser reports a certificate, privacy or connection error.
Automatic download	A page asks to install an app, profile, certificate or “security update”.
Too much information	A café network requests card details, a one-time code or identity documents.
Pressure	The page says access will be blocked unless you act immediately.

If the request does not make sense for free Wi-Fi, close the page and disconnect.



Before, during and after using public Wi-Fi

BEFORE

Confirm the exact network name with staff. Turn off auto-join and file sharing.

WHILE CONNECTED

Use mobile data for banking, payments and sensitive work. Do not ignore browser warnings.

IF YOU ENTERED DETAILS

Disconnect, change the affected password from a trusted connection, sign out active sessions and enable MFA.

Best protection Use MFA or passkeys, keep devices updated, and use 4G/5G or your own hotspot for sensitive activity.

A familiar Wi-Fi name is not proof. Verify first, then connect.

Routes into cybersecurity

No single starting point

Customer service, IT support, policing, retail, analysis and apprenticeships can all build relevant skills.

Skills employers notice

Curiosity, communication, problem solving, teamwork and calm decision-making.

Practical first steps

Try Cisco Networking Academy, Microsoft Learn, TryHackMe beginner paths, local colleges and cyber apprenticeships.

Your route does not need to look like anyone else's.





Three tracks to remember

1. **Pause before acting**
2. **Verify using a different route**
3. **Tell someone and report it**

Questions?

Thank you for joining the playlist.