

SLIDE OUTLINE · GRADES 9-12 · 9 SLIDES

Account takeover

An editable PowerPoint version of these slides is included in the lesson pack.



Account takeover

- How accounts get hijacked
- How to lock them down
- How to get one back

SLIDE 1 · SPEAKER NOTES

Set a no-blame tone. Most takeovers come from a reused password or a shared code, and both are fixable.



How takeovers happen

- Password reuse and credential stuffing
- Phishing kits: fake login pages that relay your code
- The code trick: 'I sent my code to you by mistake'
- SIM swap: your number moved to their phone

SLIDE 2 · SPEAKER NOTES

Credential stuffing in one line: a leak from one site gets tried on many others by software. Phishing kits can capture a code and use it in real time, which is why a request for a code proves nothing.



Passwords that hold up

- Long passphrases: four or more random words
- A different one for every account
- A password manager remembers them for you
- Email gets your strongest password

SLIDE 3 · SPEAKER NOTES

Explain that the password manager's main password should be a long passphrase only the student knows. Email is the master key because it resets everything else.



The MFA ladder

- Strongest: passkeys and security keys
- Strong: authenticator app with number matching
- Good: authenticator app codes
- Weakest: text or email codes, still far better than none

SLIDE 4 · SPEAKER NOTES

Passkeys only work on the real site, so a fake page has nothing to capture. Text codes can be phished or redirected by a SIM swap. Never tell students to turn MFA off.



Plan recovery before you need it

- Save recovery codes somewhere safe and offline
- Keep your recovery email and phone current
- Know the official recovery page
- Add a PIN to your phone carrier account

SLIDE 5 · SPEAKER NOTES

These steps take five minutes now and save days later. Students can do them at home with a family member.



Tabletop: Sam was hijacked

- Roles: Owner, Tech lead, Communications lead, Recorder
- 10 minutes: Contain, Recover, Protect, Tell
- New inject every 2 minutes

SLIDE 6 · SPEAKER NOTES

Read the opening card aloud. Flip injects on time even if groups are not done. That pressure is realistic and drives the discussion.



A strong recovery plan

- Contain: secure email first from a trusted device
- Recover: official recovery page only
- Protect: new unique passwords, strongest MFA
- Tell: friends, platform, trusted adult, help desk for school accounts

SLIDE 7 · SPEAKER NOTES

Use this slide during the debrief to compare plans. Highlight any group that warned friends early.



Red flags during recovery

- 'Pay me and I will restore your account'
- Anyone asking for a code
- Links in DMs claiming to be the security team

SLIDE 8 · SPEAKER NOTES

People who were just hacked are prime targets for a second scam. Only the official help center or recovery page is safe.



Your move this week

- Unique passphrase or password manager for email
- Turn on the strongest MFA offered
- Save recovery codes
- Threats or blackmail? Tell a trusted adult right away

SLIDE 9 · SPEAKER NOTES

Point to the help desk and counselor names on the board. Nobody gets in trouble for asking for help.