

CLASSROOM LESSON · GRADES 9-12

Account takeover

How accounts get hijacked, how to lock them down and how to get one back

Students learn the five common routes to account takeover (password reuse and credential stuffing, phishing kits, one-time-code tricks and SIM swaps), compare defenses from passphrases and password managers to app-based MFA, number matching and passkeys, then run a tabletop exercise: a friend's account was hijacked and their group has 10 minutes to build a recovery plan as new problems arrive.



GRADE BAND
9-12

TIME
50 minutes

FORMAT
Whole class + groups

PREP
Print & cut, ~10 min

BIG IDEA



Most account takeovers start with a reused password or a code someone was tricked into sharing; unique passwords, strong MFA and a recovery plan made in advance turn a disaster into a bad afternoon.



Students will be able to

- ☐ Explain in plain words how password reuse, credential stuffing, phishing kits, one-time-code social engineering and SIM swaps lead to account takeover
- ☐ Rank MFA options from strongest to weakest (passkeys and security keys, authenticator apps with number matching, app codes, text or email codes) and explain the tradeoff of each
- ☐ Build a step-by-step recovery plan for a hijacked account that secures email first, uses only official recovery routes and warns contacts
- ☐ Create a personal prevention plan: unique passphrases or a password manager, the strongest MFA available and saved recovery codes



Materials

- Projector or board for the slide outline
- Worksheet 1: Takeover scenarios (1 per student)
- Worksheet 2: Match the term (1 per student)
- Tabletop packet per group of 4: the scenario cards cut apart, with the five cards marked 'Inject' kept face down in order
- Chart paper or a shared document per group for the 10-minute recovery plan
- A visible timer (phone, board timer or projector)

Before class

- Print the worksheets and one card set per group. Put the five Inject cards (Inject 1 through Inject 5) in a separate envelope in order.
- Write the plan headings on the board: Contain, Recover, Protect, Tell.
- Write your district help desk contact for school accounts on the board, plus the counselor's name for anything involving threats or blackmail.
- Optional: check whether your school's student accounts support an authenticator app or passkeys so you can mention the real options. Do not ask students to change school account settings in class unless your technology team has approved it.



Vocabulary

- **Account takeover** — When someone else gets control of your account, changes the password or recovery details and uses it as you.
- **Password reuse** — Using the same password, or a small variation, on more than one account. One leak then unlocks several accounts.
- **Credential stuffing** — Attackers take usernames and passwords leaked from one site and use software to try them on many other sites, hoping people reused them.
- **Phishing kit** — A ready-made package of fake login pages that copy real sites. Some pass your password and code to the real site instantly, so the attacker logs in as you.

Vocabulary (continued)

- **One-time code** — A short code sent by text, email or app to confirm a login. It is only for you. Anyone asking for it is trying to get into your account.
- **SIM swap** — A criminal tricks a phone carrier into moving your phone number to their device, so your calls and text codes go to them.
- **Multifactor authentication (MFA)** — Logging in with two or more kinds of proof, such as a password plus an app approval, a security key or a fingerprint.
- **Number matching** — An MFA approval where you type the number shown on the login screen into your authenticator app, which stops you from approving a login you did not start.
- **Passkey** — A login based on FIDO standards that uses your device's unlock (face, fingerprint or PIN) instead of a password. It only works on the real site, so a fake page cannot capture it.
- **Recovery codes** — Backup codes a site gives you when you turn on MFA, to get back in if you lose your phone. Store them somewhere safe and offline.

Standards alignment

- **ISTE Standards for Students 1.2.d** — Digital privacy (paraphrased): students take action to protect their privacy on their devices and manage their personal data and account security online.
- **ISTE Standards for Students 1.2.a** — Digital footprint (paraphrased): students manage their digital identity and understand how what happens to their accounts affects them and the people they are connected to.
- **CSTA PK-12 Computer Science Standards (2026) HS-SYS-SE-31** — Paraphrased: identify different cybersecurity and physical security measures and the tradeoffs they create for users, data and devices, such as MFA adding security but some inconvenience.
- **CSTA PK-12 Computer Science Standards (2026) HS-SYS-SE-32** — Paraphrased: classify the causes and impacts of security breaches and social engineering attacks for individuals and other groups.
- **CSTA PK-12 Computer Science Standards (2026) HS-SYS-SE-33** — Paraphrased: propose a high-level solution to a security flaw in a described scenario, including technical and non-technical steps.
- **CSTA K-12 Computer Science Standards (2017) 3A-NI-06** — Paraphrased: recommend security measures for different scenarios based on how efficient, practical and ethical they are.
- **CSTA K-12 Computer Science Standards (2017) 3A-NI-07** — Paraphrased: compare security measures, weighing usability against security.

Aligns with commonly used digital citizenship frameworks (ISTE Standards for Students) and with both the 2026 CSTA PK-12 and the 2017 CSTA K-12 computer science standards; Georgia districts can map it to their state computer science, cybersecurity pathway and digital literacy expectations.

Lesson sequence · 50 minutes

5' Warm-up

- 1 Show slide 1. Ask students to think, not answer aloud: How many accounts do you have? How many different passwords?
- 2 Ask for a show of hands: Who knows someone whose account got hacked? What happened first? Collect the symptoms on the board (posts they did not make, locked out, friends getting strange DMs).
- 3 Frame the lesson: we will learn how it happens, how to lock it down and how to get it back.

Say: *Getting hacked usually is not about being bad with technology. It is mostly about one old password or one code shared in a moment of panic. That is good news, because both are fixable.*

12' Mini-lesson

- 1 Slide 2, How takeovers happen (4 minutes): password reuse and credential stuffing (a leak from one site gets tried everywhere); phishing kits (fake login pages that can pass your password and code to the real site in real time); the code trick ('I sent my code to you by mistake'); SIM swap (your number moved to a criminal's phone, so text codes go to them).
- 2 Slide 3, Passwords (2 minutes): long passphrases of four or more random words, a different one for every account, and a password manager to remember them. The manager's own password should be the strongest one you have.
- 3 Slide 4, MFA ladder (4 minutes): strongest are passkeys and security keys, because they only work on the real site; then authenticator apps with number matching; then app codes; weakest are text or email codes, which can be phished or redirected by a SIM swap, but they are still far better than nothing.
- 4 Slide 5, Recovery planning (2 minutes): secure your email first because it resets everything else, save recovery codes, keep your recovery phone and email up to date, and know the official recovery page before you need it.

Say: *Think of your email account as the master key. If someone gets your email, they can click 'forgot password' on almost everything else. So email gets your best password and your strongest MFA.*

18' Activity

- 1 Tabletop setup (3 minutes): groups of 4 take roles: Account owner (Sam, a fictional junior), Tech lead, Communications lead and Recorder. Read the opening card aloud: Sam's social account is posting ads to all followers, the password no longer works and the recovery email was changed to one Sam does not recognize.
- 2 Recovery plan clock (10 minutes): groups write a plan under the four headings Contain, Recover, Protect and Tell. Every 2 minutes, flip the next Inject card (Inject 1 through 5). Each inject adds a new problem the group must fit into the plan.
- 3 Gallery check (3 minutes): groups post their plans. Each group places a check mark beside one step on another group's plan that they missed.
- 4 Debrief the injects with the class (2 minutes), using the model answers on the cards.

Say: *You are Sam's friends. You have 10 minutes. Real recovery is messy, so new problems will land on your table every 2 minutes. Write steps in order, and name who does what.*

8' Discussion

- 1 Ask which inject changed each group's plan the most and why. Usually it is the reused email password or the SIM swap.
- 2 Use two or three discussion questions, including the tradeoff of text codes versus no MFA at all.
- 3 Make clear that if a takeover involves threats, blackmail or money, students should tell a trusted adult right away. Nobody gets in trouble for asking for help.

7' Exit ticket

- 1 Students complete Worksheet 2 (Match the term) individually as a quick check, about 4 minutes.
- 2 Students answer the three exit ticket questions on a half sheet, about 3 minutes. Worksheet 1 and the family sheet go home.

Discussion questions

1. Sam used the same password for social media and email. Why did that turn one hacked account into many?

Listen for: Once the attacker had the email, they could use 'forgot password' to reset other accounts. Students connect reuse to credential stuffing and explain why email deserves a unique password and the strongest MFA.

2. Text-message codes can be phished or redirected by a SIM swap. Should people still use them?

Listen for: Yes, if that is the only option, because text codes are far better than no MFA. Strong answers add: switch to an authenticator app, number matching or a passkey when the site offers it, and add a PIN to the phone carrier account.

3. Why does a passkey protect you even if you click a convincing phishing link?

Listen for: A passkey is tied to the real website and there is no reusable password to type, so a fake site has nothing it can capture and replay.

4. Someone DMs Sam offering to 'recover the account for \$50.' What is going on?

Listen for: A second scam. Only use the platform's official recovery page or help center, never paid 'recovery' offers in DMs.

5. What is the tradeoff of MFA, and how would you convince a friend it is worth it?

Listen for: It adds a step and can lock you out if you lose your phone. Counter with recovery codes, a backup method and the fact that most takeovers in the lesson would have failed with strong MFA.

Exit ticket

Answer on a half sheet. No names needed.

1. Which account should you secure first after a takeover, and why? → **Email, because it can reset the passwords of almost every other account. Secure it from a device you trust, change the password and sign out all other sessions.**
2. Put these in order from strongest to weakest: text code, passkey, authenticator app with number matching. → **Passkey, then authenticator app with number matching, then text code. All are better than no MFA.**
3. Name one thing you will set up this week to prevent a takeover. → **Any specific step: a password manager, a unique passphrase for email, MFA on email or social accounts, saving recovery codes, a PIN on the phone carrier account, or deleting old accounts that reuse a password.**



Support

- Give each group a recovery plan template with the four headings and two starter steps already filled in (for example, 'Contain: secure Sam's email from a trusted device').
- Provide the MFA ladder as a printed strip students can keep on their desks.
- Assign the Recorder role to a strong writer and let other students contribute steps orally.



Extend

- Students write a one-page 'account takeover response guide' for younger students, in plain language with numbered steps.
- Research and explain, in a short paragraph, why passkeys are called phishing-resistant and what problem they still do not solve (for example, losing all your devices).
- Compare two real sites' MFA options from their help pages and recommend which method a student should choose and why, without sharing account details.



Multilingual learners

- Pre-teach the terms with simple icons: key for password, phone for SIM swap, shield for MFA, fingerprint for passkey.
- Provide sentence frames: 'First we ___ because ___.' 'This is stronger than ___ because ___.'
- Allow groups to plan in their home language and record in English with support. Share the Spanish family sheet with Spanish-speaking families.



Accessibility

- Provide worksheets and cards digitally for screen readers and in large print. Inject cards are numbered, not color-coded.
- Offer extra time or a reduced set of three injects for students who need it, and allow oral plans recorded by a partner.
- Announce each inject aloud as well as flipping the card, and keep the timer visible and audible.



Family extension

Account takeover: a family plan to lock down and recover accounts.

Today your student learned how accounts get hijacked, usually through a reused password or a login code someone was tricked into sharing, and practiced building a recovery plan for a hacked account. Families can use the same steps for their own email, banking and social accounts.

Send home the family sheet (English and Spanish) included in this lesson pack.



Follow-up: free 2-minute lesson

k12cyberforward.com/learn/account-takeover

Project it for a quick review or share the link with families.

Related Cyber Academy course: academy-students-9-12.

Sources and further reading.

- FTC — Use Two-Factor Authentication To Protect Your Accounts (breached credentials, reuse, SIM swap risk to text codes, security keys): <https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts>
- FTC — SIM Swap Scams: How to Protect Yourself: <https://consumer.ftc.gov/consumer-alerts/2019/10/sim-swap-scams-how-protect-yourself>
- FTC — What's a verification code and why would someone ask me for it?: <https://consumer.ftc.gov/consumer-alerts/2024/03/whats-verification-code-why-would-someone-ask-me-it>
- FTC — How To Recover Your Hacked Email or Social Media Account: <https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account>
- CISA — Require Multifactor Authentication (MFA methods ranked from most to least secure): <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication>
- CISA — Next Level MFA: FIDO Authentication: <https://www.cisa.gov/news-events/news/next-level-mfa-fido-authentication>
- CISA Secure Our World — Use Strong Passwords (16+ characters, passphrases, password managers): <https://www.cisa.gov/secure-our-world/use-strong-passwords>
- FIDO Alliance — Passkeys: <https://fidoalliance.org/passkeys/>
- CSTA — 2026 PK-12 Computer Science Standards: <https://csteachers.org/pk12standards/>
- ISTE Standards for Students: <https://iste.org/standards/iste-standards-for-students>