TEACHER ANSWER KEY · GRADES 9-12

Account takeover

Worksheet 1: Takeover scenarios

1. A shopping site you used in middle school announces a data breach. You used the same password there as you use for your email and your social account.

What should you do first?

- [ ] Change the shopping site password only
- [ ] Change your email password first to a new unique passphrase, then every account that shared that password, and turn on MFA ✓
- [ ] Wait to see whether anything strange happens

Change the email password first, then every account that reused it, and turn on MFA.

Leaked passwords get tried on other sites (credential stuffing). Email comes first because it can reset everything else.

2. You get a text: 'Your account is locked. Sign in here to unlock.' The page looks exactly like the real login, and after your password it asks for the code just sent to your phone.

What is most likely happening?

- [ ] A phishing kit is passing your password and code to the real site so the attacker can log in as you ✓
- [ ] The site is doing an extra security check
- [ ] The page is real because it asked for a code

A phishing kit. Close the page, open the real app yourself, and change your password if you typed it.

Asking for a code proves nothing. Fake pages can relay codes in real time. Only passkeys and security keys refuse to work on a fake site.

3. A friend's account DMs you: 'I'm locked out. The site is sending a code to your phone because you're my backup contact. Can you send it to me?'

What do you do?

- [ ] Send it, because it is your friend's account
- [ ] Send only the first three digits
- [ ] Do not send it. Contact your friend another way, such as a call or in person, and warn them their account may be compromised ✓

Do not share the code. Contact your friend by a route you already know.

The friend's account may already be taken over, and the code may be for your own account. Anyone asking for a code is trying to get in.

4. Your phone suddenly shows 'SOS only' in the middle of the day. Minutes later, a laptop at home shows an email alert that your password was changed.

What is the most likely cause, and the first move?

- [ ] A weak signal; restart the phone tomorrow
- [ ] A possible SIM swap; contact your carrier from another phone right away, then secure email from a trusted device ✓
- [ ] A phone update; ignore the email

Possible SIM swap. Call the carrier from another phone, then secure email and other accounts, and tell a trusted adult.

Losing service plus password-change alerts is a classic SIM-swap pattern. Text codes now go to the attacker, so speed matters.

5. A site offers three MFA options: text message codes, an authenticator app with number matching, or a passkey.

Which should you choose, and what should you save?

- [ ] Text codes, because they are easiest
- [ ] No MFA, because you might lose your phone
- [ ] The passkey (or the app with number matching), and save the recovery codes somewhere safe and offline ✓

Choose the passkey, or the authenticator app with number matching, and save the recovery codes.

Passkeys only work on the real site. Number matching stops accidental approvals. Recovery codes solve the lost-phone problem.

6. Your account was hijacked. A stranger DMs you: 'I work with the platform's security team. Pay $40 and I'll restore your account in an hour.'

What do you do?

- [ ] Ignore and block them, and use only the platform's official recovery page or help center ✓
- [ ] Pay, because an hour is fast
- [ ] Send your login details so they can start

Block them and use only the official recovery route. Tell a trusted adult if you were pressured to pay.

Paid 'recovery' offers in DMs are a second scam aimed at people who were just hacked.

Worksheet 2: Match the term

TERM	LETTER
1. Credential stuffing	**B**
2. Password reuse	**H**
3. Phishing kit	**G**
4. SIM swap	**F**
5. One-time code	**C**
6. Number matching	**E**
7. Passkey	**A**
8. Password manager	**D**

MEANING
A. A device-unlock login that only works on the real site and has no password to steal
B. Trying leaked usernames and passwords from one site on many other sites
C. A short login code that is only for you and should never be shared
D. A tool that creates, stores and fills a unique strong password for every account
E. Typing the number shown on the login screen into your app to approve only logins you started
F. Moving your phone number to a criminal's device so your calls and texts go to them
G. Ready-made fake login pages that can relay your password and code to the real site
H. Using the same password on more than one account, so one leak unlocks several

Scenario cards

CARD	MODEL ANSWER
1. Opening: Sam's account	From a trusted device, secure Sam's email (change password, sign out all sessions, turn on MFA); start the platform's official account recovery; warn followers from another account or through friends not to click anything. Email first stops the attacker from resetting more accounts. Official recovery is the only safe route back in.
2. Inject 1: Same password	Email is now the top priority. Change it to a unique passphrase from a trusted device, sign out all other sessions, check forwarding rules and recovery details, then turn on MFA. Whoever controls the email can reset every account linked to it.
3. Inject 2: Friends getting DMs	Tell friends by text, call or in person: do not send any codes and do not click links from Sam's account. Report the account to the platform. Hijacked accounts are used to take over friends' accounts next. Fast warnings break the chain.
4. Inject 3: No service	A parent or guardian calls the carrier from another phone right away to report a possible SIM swap, then adds a PIN to the carrier account. Change passwords again once the number is back. With Sam's number, the attacker receives text codes. The carrier is the only one who can move it back.
5. Inject 4: The recovery offer	Do not pay or reply. Block and report. Use only the platform's official recovery page. Recovery offers in DMs are a second scam aimed at people who were just hacked.
6. Inject 5: School account too	Tell the teacher and the district help desk right away so they can reset the school account and check for misuse. Nobody gets in trouble for reporting. School accounts are protected by the district technology team, and they can act faster than a student can.
7. The breach email	Assume it was a reused password. Change passwords on email and other important accounts, turn on MFA and delete the old account if you can. Leaked passwords from old accounts are tried on new ones for years.
8. Push spam at midnight	Deny every request, do not tap approve to make them stop, change your email password in the morning and switch to number matching or a passkey if offered. Repeated prompts mean someone has your password and hopes you will approve one by mistake.
9. The lost phone	Use the recovery codes you saved when you turned on MFA, or a backup method like a second device or security key. Then set up MFA on your new phone. Recovery codes and backup methods are the plan for this exact moment.
10. The password notebook	Use a password manager or long, random passphrases, a different one for each account, starting with email. Variations of one word are easy to guess once one version leaks, and sticky notes go wherever the phone goes.

Exit ticket

QUESTION	ANSWER
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.**
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.**
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.**