

FOR FAMILIES · GRADES 9-12

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.



WHAT YOUR CHILD LEARNED AT SCHOOL



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.



Try this at home

- 1 Pick each person's most important account (usually email). Turn on the strongest MFA it offers, such as an authenticator app or a passkey, and save the recovery codes somewhere safe and offline.
- 2 Agree that no one in the family ever shares a login code, even with a relative or a caller who says they are from a company.
- 3 Add a PIN or password to your mobile phone carrier account to make SIM swaps harder. Your carrier's website explains how.
- 4 Write a short family recovery card: which accounts matter most, where recovery codes are kept and who to call if a phone suddenly shows no service.



Conversation starters

- Which of your accounts would cause the most trouble if someone else controlled it?
- How many of your passwords are the same or almost the same?
- What would you do first if your account started posting things you did not write?
- Would you rather use a password manager or passphrases, and why?



Household tip

If your phone suddenly shows no service or SOS only, and you did not change anything, contact your carrier from another phone right away. It can be a sign of a SIM swap.



Watch the free 2-minute lesson together
k12cyberforward.com/learn/account-takeover

Questions? Contact your child's teacher or school office: