

PRE-PLANNING EDITION

Fresh start, fresh passphrase

Over the summer, old passwords, forgotten app accounts and stale shared folders pile up. Ten minutes of cleanup during pre-planning closes the doors scammers love to walk through in August.



1 Make it a passphrase, not a puzzle

Four or more random words beat P@ssw0rd1 every time: think 'pecan tractor library drizzle'. Long is strong. Use it for your district account only, never for shopping or streaming sites.



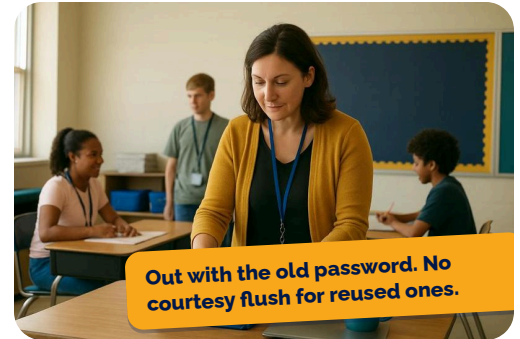
2 One account, one password

When a shopping site leaks your password, crooks try it on district email next. Give every account its own password. A district-approved password manager can remember them so you don't have to.



3 Clean out the summer junk drawer

Sign out of classroom apps you no longer use, remove last year's co-teachers from shared folders, and tell your technology team about accounts for students or staff who have left.



Spot the scam



Email

External

District IT Services <it-notice@district-k12-helpdesk.example>

Pre-planning: your password expires TODAY

Welcome back. Our records show your district password expires in 2 hours. To keep your current password and avoid losing gradebook access, confirm your username and password at k12-password-keep.example/renew. Staff who do not respond will be locked out before pre-planning ends. Thank you, IT Services Team

Spot the scam: how many red flags can you find before you flush?

Red flags I found: ○ ○ ○ ○ ○

Look for: surprise, urgency, secrecy, an unusual payment method, a sender or link you can't confirm.

FUN FACT

Federal password guidance from NIST now says systems should not force you to change passwords on a schedule, only when there is evidence one was stolen. It also says systems should allow passwords of at least 64 characters. Length wins.

Source: NIST SP 800-63B-4: Authentication and Authenticator Management



Your 60-second move

Change one reused password today, starting with district email. Make it a four-word passphrase you use nowhere else.



Who do I tell?

Name / ext. _____

Report channel _____

- ANSWER
- Five flags: the two-hour deadline, the request for your password, the strange link, the lockout threat and the nameless signature. Safe move: don't click. Go to the sign-in page you already use, or call the help desk number in the staff directory, then report the email with your report-phish button.
 - A two-hour deadline is pressure, not policy.
 - Real IT never asks you to type your password into a link in an email.
 - That web address is not your district's sign-in page.
 - A lockout threat is there to make you rush.
 - No name, ticket number or phone number you could check.



Scan for a 2-minute lesson on passphrases you'll actually remember

Free, no sign-in · k12cyberforward.com/learn