// E-SAFETY FACT SHEET

Passwords & 2FA: Lock Your Accounts

How accounts really get stolen — and the three habits that stop it

for Students, Teachers, and Parents

Almost every online problem a young person runs into — a hijacked game account, an impersonation profile, embarrassing messages sent in their name, money taken from a linked card — starts the same way: someone else got into an account. Attackers rarely “hack” anything. They log in with a password that was reused, guessed, breached, or handed over.

Two habits — a unique password for every account, and two-factor authentication turned on — stop the overwhelming majority of account takeovers.

This sheet explains how account theft actually works, gives practical steps for students, parents, and educators, and lists where to get help if an account is already compromised.

In this document:

1 Know the risks

A. Reused Passwords (the big one)

When a company suffers a data breach, the stolen email-and-password pairs get published and traded. Attackers then feed those pairs into automated tools that try them against hundreds of other sites — game platforms, social media, school portals, shopping accounts. This is called **credential stuffing**, and it works for one reason: most people reuse the same password. One breach at a site you barely remember signing up for becomes access to everything.

B. Weak and Guessable Passwords

Short passwords fall to automated guessing in seconds. So do predictable ones — a pet's name, a favourite team, a birthday, a sibling's name, a gamertag with a number on the end. Anything posted publicly on social media is a candidate. Swapping letters for symbols (P@ssw0rd) does not help; attackers' tools have accounted for that for decades. Length beats complexity.

C. Phishing — Being Asked Nicely

The simplest way to get a password is to ask for it on a page that looks legitimate. Fake login screens arrive by DM, text, or email: a "free skins" site, a "your account will be suspended" warning, a message from a friend whose account was already taken over. The page looks right, the login fails once, and by then the password is gone. Increasingly, these pages also ask for the 2FA code — and relay it in real time.

D. Sharing Passwords with Friends

Young people share account details as a gesture of trust — a streaming login, a game account, a social profile. Friendships change. Shared credentials outlive the friendship, and shared accounts are a common route to impersonation posts, deleted saves, and messages sent in someone else's name. A password given away is a password lost.

E. Weak Recovery Options

An account is only as strong as the route back into it. Security questions with answers that are public knowledge (mother's maiden name, first school, pet's name) let attackers reset a password without ever knowing it. An old, abandoned recovery email is a permanent back door. SMS codes can be intercepted through SIM-swap fraud, which is why an authenticator app is the stronger choice.

F. Devices Left Unlocked

Not every compromise is remote. An unlocked phone left on a desk gives full access to every logged-in app, plus the ability to read the 2FA codes arriving on the lock screen. Shared and school computers keep sessions alive when people forget to sign out.

→

2 What can you do?

The three rules that do most of the work

RULE 01	**Every account gets its own password.** Never reuse. If one site is breached, the damage stops there.
RULE 02	**Make it long, not clever.** Four or five random words — a passphrase — beats a short string of symbols. Aim for 16+ characters.
RULE 03	**Turn on two-factor authentication (2FA)** everywhere it's offered, starting with email. An app code or security key beats an SMS code.

For students

- Use a **password manager** — built into your browser or phone, or a dedicated app. It generates and remembers unique passwords so you don't have to. Protect it with one strong passphrase you actually memorise.
- **Secure your email first.** Email is the master key: whoever controls it can reset every other account. Strong unique password plus 2FA, today.
- Prefer an **authenticator app** over text-message codes. Save the backup codes somewhere safe — offline is fine.
- **Never type a password on a page you reached from a link.** Navigate to the site yourself, or use your app.
- No real service will ever ask for your password or 2FA code in a chat, DM, or voice call. Not moderators, not admins, not "support".
- Don't share logins — not with best friends, not with teammates, not for a trade.
- Give **fake answers to security questions** and store them in your password manager. The answer doesn't have to be true, it has to be unguessable.
- Lock your phone with a PIN, pattern, or biometric, and hide message previews on the lock screen.

For parents & caregivers

- Set up a password manager as a household tool, and model using it. Kids copy what adults actually do, not what they're told.
- Walk through enabling 2FA together on the accounts that matter most: email, then game platforms, then social media.
- Remove saved payment cards from game and app stores, or require a password for every purchase.
- If an account is compromised, respond calmly. Kids who expect to lose the device or the game hide the problem instead of reporting it.

For teachers & schools

- Teach passphrases over "complexity rules" — current NIST guidance favours length and screening against breached passwords over forced symbols and frequent expiry.
- Make 2FA setup a hands-on lesson, not a slide. Students should leave having actually enabled it on one account.
- Remind students to sign out of shared and library machines, and to lock screens when stepping away.
- Frame it as professional practice: identity and access management is a full career field, not a chore.

Career link. Protecting credentials is the daily work of identity and access management, and of the analysts who investigate account takeovers. See where these skills lead at getintocyberjobs.com.

→

3 Resources and where to get help

If an account has already been taken over

STEP 01	Change the password from a **different, trusted device** — and change your email password first.
STEP 02	Turn on 2FA, then **sign out all other sessions** (most platforms have a "log out everywhere" option).
STEP 03	Check recovery settings for anything the attacker added — unfamiliar phone numbers, forwarding rules, backup emails, connected apps.
STEP 04	Change the password anywhere else that password was used. Then warn friends, because the account will have been used to message them.
STEP 05	If money or card details were involved, contact the bank and report it. Keep screenshots.

- **Have I Been Pwned** — free, reputable check for whether your email appears in a known data breach: haveibeenpwned.com
- **CISA Secure Our World** — plain-language federal guidance on passwords, 2FA, and phishing: cisa.gov/secure-our-world
- **FTC consumer advice** — what to do after a data breach or account compromise: consumer.ftc.gov
- **IdentityTheft.gov** — federal recovery plans if personal information or money was taken: identitytheft.gov
- **Report fraud** to the FTC at reportfraud.ftc.gov, or to the FBI's Internet Crime Complaint Center at ic3.gov
- **Practice the skill** — free phishing-detection game: gamingforlearning.com

// Warning signs an account is compromised

- Login alerts or password-reset emails you didn't request
- Friends receiving messages or links you didn't send
- Posts, follows, or purchases you don't recognise
- Being logged out unexpectedly, or a password that suddenly stops working
- Missing in-game items, currency, or skins
- New devices or unfamiliar locations in your account's security activity

A password-reset email you didn't ask for is not spam — it usually means someone is actively trying to get in. Act on it the same day.