threat level: human

The attack vector you can't patch.

Passwords, MFA and Account Takeover

How accounts get stolen, and the three habits that stop almost all of it.

99%+
of identity attacks stopped by phishing-resistant MFA
Microsoft, 2025

88%
of web-app attacks use stolen credentials
Verizon DBIR, 2025

17B+
accounts exposed in known data breaches
Have I Been Pwned, 2026

HOW ACCOUNTS GET TAKEN OVER

01 Reused passwords
One leaked password unlocks every other account that shares it.

02 A login reached through a link
Adversary-in-the-middle pages relay your real login and steal the session token.

03 An MFA prompt you did not start
Approving a push you did not request hands over your live session.

HARDEN YOUR ACCOUNTS

04 Use a password manager
A long, unique password per site, so one breach cannot spread.

05 Prefer phishing-resistant MFA
An app code, a passkey, or a security key beats a code sent by SMS.

06 Check your exposure
Look up your email in known-breach data and reset anything that shows up.

SIGNS AN ACCOUNT IS ALREADY TAKEN

07 Logins or alerts you do not recognize
Sign-in notices from new devices or locations you never used.

08 Settings that changed on their own
New forwarding rules, recovery emails, or phone numbers added to the account.

09 Contacts getting messages you did not send
Spam or scam messages going out from your account.

DO / DON'T

DO

- Use a password manager so every account has a long, unique password.
- Turn on phishing-resistant MFA: a passkey, a security key, or an app code over SMS.
- Check your email and passwords against known-breach data and reset matches.
- Keep recovery email and phone current, and review active sessions now and then.

DON'T

- Do not reuse passwords across sites.
- Do not enter your password on a page you reached from a link.
- Do not approve an MFA prompt you did not start, and never share a one-time code.
- Do not rely on SMS codes alone for your most important accounts.

THE ONE MOVE

Turn on multi-factor authentication everywhere, use a password manager so every login is unique, and never approve an MFA prompt you did not personally trigger. Those three habits stop most account takeovers.

IF IT HAPPENS

1. From a clean device, change the password and sign out all sessions.
2. Re-check MFA, recovery options, and forwarding rules for anything you did not set.
3. Reset every other account that shared that password.
4. Warn contacts if scam messages went out, and report platform takeovers to the provider.

Get a briefing like this every week, free.

threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: Microsoft Digital Defense Report (2025); Verizon DBIR (2025); Have I Been Pwned (2026). Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.