What is account takeover?

Account takeover (ATO) is when an attacker gains control of a legitimate user account, usually through phishing, credential stuffing, or password cracking. Because they then hold valid credentials, their actions blend into normal use and raise few alarms. The defenses are multi-factor authentication (ideally phishing-resistant), unique passwords, detection of anomalous logins, and fast session revocation.

HOW IT WORKS

01 Why account takeover is so dangerous

A valid login is the quietest way into a company. Nothing is exploited, no malware runs, and to your systems it looks like the real user arriving for work.

Email accounts are the worst to lose, because email is the reset mechanism for everything else, so one mailbox can unlock a dozen other accounts. From any foothold, an attacker can read data, move money, impersonate the user to colleagues, and pivot toward more valuable systems, all under a trusted name.

02 Signs of account takeover

The tell-tale signs include logins from unfamiliar locations or devices, new mailbox rules or auto-forwarding (attackers hide their tracks by filtering replies), changes to multi-factor settings or recovery details, and unusual sends, purchases, or transactions from the account. Detection depends on watching authentication and account-change events, not just failed logins.

HOW TO DEFEND

- Multi-factor authentication, so a stolen password is not enough. Phishing-resistant methods (passkeys or hardware keys) also defeat real-time proxy phishing and prompt bombing.
- Unique passwords in a password manager, so a leak elsewhere does not open your door.
- Block known-breached passwords at sign-up and reset.
- Detect anomalous logins and step up authentication when something looks off.
- Revoke sessions fast when an account is suspected, and limit what any one account can reach.

SOURCES

[1] Valid Accounts (Technique T1078)

[2] Cyber Threats and Advisories

[3] Digital Identity Guidelines (SP 800-63B)

Find out what one stolen login could reach in your environment.

securelayer7.net/learn/threats/account-takeover

Open online