A

Account Hijacking: Warning Signs and Complete Recovery Steps

Account hijacking can survive a password change through sessions, forwarding rules, OAuth grants, or recovery changes. Use this ordered recovery checklist.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

Account hijacking, also called **account takeover (ATO)**, is unauthorized control of an online account. It can affect email, social media, banking, shopping, cloud, payroll, gaming, and workplace identities. Attackers may steal money or data, impersonate the owner, reset linked accounts, or use the trusted account to target contacts.

When access came from a stolen session rather than a password, review session hijacking as well. An already authenticated token can remain useful to an attacker until the service invalidates it, which is why session revocation belongs in the recovery process.

Changing the password is important, but it is not always enough. A hijacker may still have an active session, a malicious email-forwarding rule, an OAuth app grant, an app password, or altered recovery details.

How accounts are hijacked

- **Phishing:** a fake sign-in page captures credentials and sometimes an MFA code.
- **Password reuse:** attackers test credentials leaked from another service, known as credential stuffing.
- **Information stealers:** malware takes saved passwords, browser cookies, and session tokens.
- **Session theft:** a stolen cookie can bypass the normal password and sometimes MFA until the session is revoked.
- **MFA abuse:** repeated prompts, SIM swapping, or social engineering tricks the victim or support staff.
- **Malicious app consent:** a user authorizes an OAuth application to read mail or files without giving it the password.
- **Recovery compromise:** attackers control the recovery email, phone number, backup codes, or an already-compromised primary mailbox.

Warning signs

- login alerts, devices, locations, or sessions you do not recognize;
- password, MFA, recovery email, or phone changes you did not make;
- messages, purchases, posts, transfers, or password resets you did not initiate;
- contacts receiving requests for money, codes, or files from your account;
- missing email, unfamiliar forwarding or inbox rules, delegates, filters, or app passwords;
- being locked out even though the password was recently changed.

Recovery steps if you can still sign in

1. **Use a known-clean device.** Update and scan the device first if malware or a malicious browser extension may have captured the account.
2. **Secure the primary email account first.** It can reset most other accounts. Then protect the password manager, mobile carrier, financial services, and work identity.
3. **Change to a unique password.** Do not make a small variation of the old one. Update every other account that reused it.
4. **Sign out everywhere.** Revoke all sessions, remembered devices, refresh tokens, app passwords, and backup codes when the provider offers those controls.
5. **Repair security settings.** Remove unknown MFA methods and recovery contacts, generate fresh backup codes, and enable a passkey or phishing-resistant MFA where available.
6. **Remove hidden access.** Review connected OAuth apps, third-party integrations, email forwarding, inbox rules, delegates, filters, and automatic replies.
7. **Review activity and damage.** Check sent and deleted mail, orders, ads, payment methods, posts, cloud sharing, login history, and linked accounts. Warn affected contacts through another channel.

What to do if you are locked out

Use the provider's official account-recovery page reached from its app or a manually typed domain. Provide previous passwords, known devices, purchase records, or other proof the provider requests. Do not pay a stranger who promises guaranteed recovery; “account recovery agents” on social media are often a second scam.

For email and social accounts, the U.S. FTC provides a concise official recovery checklist. For a workplace account, contact the internal help desk or security team immediately rather than trying to investigate alone.

If money, identity, or work data is involved

- Call the bank, card issuer, payroll team, or mobile carrier using verified contact information. Freeze or reverse transactions when possible.
- Save timestamps, alerts, transaction IDs, headers, screenshots, and support case numbers.
- Report identity theft or fraud through the relevant national reporting service and consider a credit freeze where available.
- In an organization, revoke enterprise sessions, preserve identity and mailbox logs, search for malicious rules and app consent, and review actions performed by the account.

How to prevent account takeover

- Use a password manager and a different long password for every service.
- Prefer passkeys, security keys, or authenticator-based MFA over SMS when supported.
- Never approve an unexpected MFA prompt; report it and change the password.
- Review active sessions, recovery methods, connected apps, and email rules periodically.
- Keep devices and browsers updated, and avoid installing cracks or unknown extensions.

Account hijacking FAQ

Why did the attacker return after I changed my password?

An existing session, OAuth grant, forwarding rule, malware infection, or compromised recovery method may still provide access.

Which account should I recover first?

Usually your primary email, because it controls password resets. Immediate financial or workplace risk may require parallel calls to the bank or security team.

Does MFA make takeover impossible?

No, but phishing-resistant MFA and passkeys greatly reduce common attacks. Session theft and malicious app consent still require careful review.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com