A

Account Compromise: Warning Signs, Recovery, and Prevention

Account compromise means someone gained unauthorized access or control. Changing the password matters, but sessions, recovery methods, apps, and hidden rules also need review.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

An **account compromise** occurs when someone gains unauthorized access to an online account or its active session. The attacker may know the password, hold a stolen session token, control a recovery method, have an authorized third-party app, or already be signed in on another device.

Changing a password is important, but it may not remove every form of access. Recovery should secure the account, the device used to access it, connected services, and any people or money affected.

Warning signs

- a sign-in, device, location, password reset, or MFA prompt you do not recognize;
- changed password, recovery email, phone number, MFA method, passkey, or security key;

- messages, posts, files, advertisements, purchases, or transfers you did not create;
- new forwarding rules, mail delegates, filters, API tokens, app passwords, or connected applications;
- missing messages, security alerts moved to trash, or contacts receiving unusual requests;
- access suddenly denied while the account still appears active to other people.

A location can be approximate and a familiar device name can be reused, so confirm with timestamps, IP information, activity, and provider alerts rather than one field alone.

Recovery checklist

1. **Use a known-clean device.** Update it and scan for malware if the original device may have a credential stealer or hostile extension.
2. **Use the provider's official recovery page.** Navigate from a saved bookmark, app, or independently typed address—not a link in an alert message.
3. **Secure the password.** Set a new, unique password and change it anywhere the old password was reused.
4. **Revoke access.** Sign out other sessions and revoke refresh tokens where the provider offers that control. A password reset may not invalidate every token or app password.
5. **Repair account security.** Remove unknown recovery addresses, phone numbers, MFA methods, passkeys, devices, app passwords, and trusted browsers.
6. **Remove hidden persistence.** Review connected OAuth apps, delegates, mailbox forwarding and filters, API keys, social integrations, and administrator roles.
7. **Review activity and damage.** Check sent and deleted items, file sharing, payment methods, purchases, ads, security settings, downloads, and linked accounts.

Google's official compromised-account guidance includes reviewing security events, devices, recovery settings, connected apps, forwarding rules, and product-specific activity.

If you cannot sign in

Start the provider's account-recovery process promptly, ideally from a familiar device and network. Supply accurate historical information and preserve case numbers. Do not pay strangers who claim they can recover an account or ask for passwords, one-time codes, backup codes, remote access, or cryptocurrency.

If the account belongs to an employer, school, or customer organization, contact its administrator through a known channel. Administrators may be able to disable access, preserve logs, restore settings, and verify identity.

Limit follow-on harm

- secure email first because it can reset many other accounts;
- contact the bank or payment provider immediately about unauthorized transactions;
- warn contacts through another channel if the attacker sent messages or files;
- check other accounts for password reuse and suspicious password-reset messages;
- report identity theft, impersonation, or financial fraud to the appropriate provider and authority.

For organizational accounts

Preserve authentication, mailbox, endpoint, application-consent, privilege, and data-access logs before retention expires. Revoke sessions, disable risky access, remove attacker-added methods and applications, rotate exposed user and service credentials, and determine what data or actions were accessible. Search for related accounts and the original phishing or malware vector.

Microsoft's current email-account response specifically calls out session revocation, MFA methods, application consent, and mailbox changes.

Prevention

- use unique passwords stored in a trusted password manager;
- prefer passkeys or phishing-resistant MFA and keep recovery codes offline;

- deny unexpected MFA prompts and report repeated prompts;
- review connected apps, devices, recovery methods, and forwarding periodically;
- keep devices and browsers updated and limit extensions;
- verify sign-in pages independently and never share one-time or recovery codes.

Account compromise FAQ

Is changing the password enough?

No. Revoke sessions and tokens and review recovery methods, MFA, devices, connected apps, rules, and activity.

Should I delete the account?

Usually secure and investigate it first. Immediate deletion can destroy evidence, disrupt recovery, and leave linked accounts exposed.

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