GRIDINSOFT

HELP CENTER

OFFICIAL SUPPORT GUIDE

C

Credential Harvesting: Signs and Prevention

What it is Credential harvesting is the collection of usernames, passwords, authentication tokens, session cookies, or other data that can be used to access accounts. Attackers may gather credentials through fake sign-in pages, malicious...

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 17, 2026	2 min

What it is

Credential harvesting is the collection of usernames, passwords, authentication tokens, session cookies, or other data that can be used to access accounts. Attackers may gather credentials through fake sign-in pages, malicious software, compromised databases, browser theft, or social engineering. The goal is unauthorized access, fraud, or a path deeper into an organization.

How it works

A phishing link can copy a familiar login page and send entered details to the attacker. Malware can read browser storage, intercept keystrokes, or extract credentials from memory. Stolen credentials are then tested against email, cloud, VPN, and financial services, often from infrastructure chosen to resemble normal user activity.

Key points

- Multi-factor authentication reduces risk, but stolen session cookies and convincing approval prompts can bypass weak implementations.
- Password reuse turns one exposed account into access to several unrelated services.
- Successful sign-in logs may look normal unless device, location, timing, and session behavior are reviewed together.

What to do

- Reset the affected password from a clean device and revoke active sessions and application tokens.
- Enable phishing-resistant MFA where available and remove unfamiliar recovery methods.
- Inspect the endpoint for infostealers before entering replacement credentials.
- Notify administrators quickly so they can search for mailbox rules, forwarding, and lateral movement.

If credentials were entered

Open the real service from a known bookmark, change the password, revoke all sessions, and inspect recovery email, phone, forwarding, API token, and MFA settings. Reset reused passwords on other services and alert the account owner or security team. Preserve the lure URL, sender, time, and screenshot without revisiting it. Password changes made on an infected device may also be captured, so use a clean system. Most harvesting begins with phishing; phishing-resistant MFA and a password manager reduce both successful entry and reuse.