P

Password Sniffer: Credential Capture, Detection, and Response

Password sniffer is an informal term for tools that capture credentials. Learn when network traffic exposes passwords and how other credential-stealing methods differ.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What network password sniffing means

02 What encryption protects

03 Other methods confused with password sniffing

04 Signs to investigate

05 How to respond to possible credential capture

06 Prevention

07 Frequently asked questions

Quick answer: A password sniffer is an informal term for software or hardware used to capture login credentials. Strictly, network sniffing observes data moving across a network and can expose passwords sent through insecure protocols. Credentials can also be stolen through keylogging, phishing, browser stores, memory, or malicious authentication components; those methods are not packet sniffing even when people use the same label.

01 What network password sniffing means

A network sniffer captures packets available to the device or sensor. Administrators legitimately use packet capture to troubleshoot networks and investigate incidents. It becomes malicious when someone collects traffic without authorization or searches it for credentials and sensitive data.

MITRE ATT&CK describes this behavior as Network Sniffing (T1040). An attacker may sniff from a compromised endpoint, router, virtual host, network appliance, or cloud network component. On a switched network, a normal workstation does not automatically see all other traffic; the attacker may need control of network infrastructure, port mirroring, address-resolution manipulation, a rogue access point, or another position in the path.

02 What encryption protects

Properly validated TLS protects the contents of HTTPS and other encrypted connections while data is in transit. A passive observer may still see metadata such as IP addresses, timing, sizes, and often DNS information, but not the password inside a correctly encrypted request. Warnings about an invalid certificate matter because accepting an impostor certificate can defeat that protection.

Encryption in transit does not protect credentials before they are encrypted on the endpoint or after they are processed by a compromised service. Malware can record keystrokes, read browser data, steal session tokens, access process memory, or modify a login page. Saying that “HTTPS prevents password theft” is therefore too broad; it prevents passive reading of the protected network payload, not every credential attack.

03 Other methods confused with password sniffing

- **Keylogging:** records keys or input events before an application sends them.
- **Phishing:** persuades a person to submit a password to a fraudulent page or prompt.
- **Browser and password-store theft:** extracts saved credentials, cookies, or tokens from files, databases, extensions, or operating-system stores.
- **Memory credential theft:** accesses secrets or reusable authentication material held by a process or operating system.
- **Authentication interception:** inserts malicious code, a proxy, or a rogue identity component into the login flow.
- **Credential stuffing:** tries passwords leaked from another service; it does not capture a new password from the victim's network.

The distinction matters because evidence and remediation differ. Replacing a router will not remove a keylogger, and cleaning one laptop will not correct a compromised identity provider.

04 Signs to investigate

- Packet-capture tools, promiscuous-mode interfaces, unexpected network drivers, or capture files on an unauthorized system.
- ARP or DNS changes, duplicate gateways, rogue wireless access points, or certificate warnings.
- Unusual access to browser profiles, password stores, authentication processes, or credential-related memory.
- New root certificates, proxies, VPN profiles, extensions, keyboard hooks, or accessibility permissions.
- Successful account access from unfamiliar devices or locations, unexpected MFA prompts, token reuse, or mailbox rules.

No single symptom proves a password sniffer. Capture endpoint process and persistence data, network configuration, certificates, authentication logs, identity-provider events, and the time of suspected exposure.

05 How to respond to possible credential capture

1. **Isolate the suspected device or network component.** Preserve it for investigation when business impact permits.
2. **Use a known-clean device.** Do not change passwords from the potentially monitored endpoint.
3. **Secure the primary identity first.** Reset email or single sign-on credentials, revoke active sessions and refresh tokens, and review MFA methods and recovery contacts.
4. **Rotate affected secrets.** Include reused passwords, service accounts, API keys, VPN credentials, and certificates according to the likely capture scope.
5. **Find and remove the capture path.** Investigate endpoints, network infrastructure, proxies, wireless access, browser components, and identity systems rather than merely deleting one visible tool.
6. **Review account activity.** Look for data access, forwarding rules, changed permissions, new devices, and transactions during the exposure window.

A password reset alone may not invalidate stolen session cookies or API tokens. Explicitly revoke sessions and keys. If privileged credentials were captured, widen the incident scope and rebuild systems whose integrity cannot be established.

06 Prevention

Disable plaintext authentication protocols and require TLS with valid certificate verification. Use secure Wi-Fi and network access controls, protect switch, router, hypervisor, and cloud-network administration with MFA, and restrict who can run packet capture. Segment sensitive systems and monitor configuration changes.

Use phishing-resistant MFA where possible because stolen passwords alone then have less value, while recognizing that some session and real-time phishing attacks can bypass weaker MFA. Keep browsers and operating systems updated, allow only trusted extensions, use managed password storage, and deploy endpoint detection around credential-access behavior. Unique passwords prevent one captured password from unlocking unrelated accounts.

07 Frequently asked questions

Can someone read my password just because we share Wi-Fi?

Not from properly encrypted, certificate-validated HTTPS traffic by passive listening alone. Risk rises with plaintext protocols, certificate bypass, a rogue access point, or a compromised endpoint.

Is Wireshark a password sniffer?

Wireshark is a legitimate packet-analysis tool. Authorization and use determine whether a capture is appropriate; it cannot magically decrypt correctly protected traffic.

Should I only change the exposed password?

No. Revoke sessions and tokens, secure recovery methods, rotate any reused or accessible secrets, and remove the underlying capture mechanism.

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