GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

B

Banking Trojan: How It Steals Money and How to Respond

A banking Trojan is malware designed to steal financial credentials, manipulate online banking sessions, or enable fraudulent transactions.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

CONTENTS

In this guide

01 How banking Trojans work
02 Common capabilities
03 How infection happens
04 Warning signs
05 What to do immediately
06 Prevention
07 Banking Trojan versus phishing
08 Source

Quick answer: A banking Trojan is malware designed to steal access to bank or payment accounts, manipulate financial sessions, or enable fraudulent transactions. It may capture keystrokes, alter pages inside the browser, display fake overlays, steal cookies, intercept codes, or give an attacker remote control. Stop banking on the affected device, isolate it,

and contact the financial institution immediately.

01 How banking Trojans work

A Trojan pretends to be legitimate or arrives through another deceptive path. Banking-focused families then watch for financial sites or apps and activate credential or transaction theft. Some older and desktop families used browser hooks and web injections. Mobile banking malware often abuses accessibility services, screen overlays, notification access, or SMS permissions. Other families begin as banking Trojans but evolve into general loaders or remote-access platforms.

The browser padlock and HTTPS do not stop malware already operating on the endpoint. A web injection can change what the user sees before information is encrypted for transmission, while remote-control malware can submit a transaction through the genuine session.

02 Common capabilities

- **Credential capture:** keylogging, form grabbing, fake login fields, overlays, or screenshots.
- **Session theft:** stealing browser cookies or tokens to reuse authenticated access.
- **Transaction manipulation:** changing beneficiary or payment details while showing expected information to the victim.
- **Code interception:** reading notifications or SMS, or prompting for a one-time code through a false page.
- **Remote access:** controlling the device, downloading modules, or hiding fraud behind the victim’s IP address.

03 How infection happens

Delivery may use phishing attachments and links, fake invoices or updates, cracked software, malicious advertisements, exploit kits, unofficial mobile apps, or another loader. On phones, attackers may impersonate a bank, government service, delivery company, or security tool and instruct the victim to grant powerful accessibility permissions.

04 Warning signs

Important signs include a security alert, a bank page requesting unusual card or identity details, repeated login or transaction errors, unfamiliar accessibility or device-administrator permissions, unknown apps or browser extensions, disabled protection, unexpected payments, new beneficiaries, and account notifications from devices or locations you do not recognize. Many infections have no visible symptoms before fraud occurs.

05 What to do immediately

1. Stop using the suspected device for banking, email, password management, or cryptocurrency.
2. Disconnect it from networks, but preserve alerts, messages, applications, URLs, timestamps, and transaction information.
3. From a clean device, call the bank using the number on the card or official site. Ask it to secure access, review pending transactions, and follow fraud procedures.
4. Change the banking and email passwords, revoke sessions, verify MFA and recovery settings, and remove unknown linked devices or applications.
5. Scan and investigate the affected endpoint. Reimage it when remote control, persistence, or high-value access may have been present.

Do not continue a call using a number shown in a suspicious message or pop-up. Do not move money to a “safe account” on an unsolicited caller’s instructions.

06 Prevention

Install apps only from official stores or verified publishers and review requested permissions. Keep devices, browsers, banking apps, and security protection updated. Use unique passwords and phishing-resistant MFA where supported. Enable transaction alerts and independent approval for unusual payments. Businesses should separate payment creation and approval, use dedicated managed devices for high-risk banking, and verify beneficiary changes out of band.

07 Banking Trojan versus phishing

Phishing can steal bank credentials without infecting a device, while a banking Trojan is software running on the endpoint. The two are often combined. If the evidence is unclear, respond to both possibilities: secure the accounts and investigate the device.

08 Source

Definitions and historical techniques are described in Europol and Check Point’s joint report, Banking Trojans: From Stone Age to Space.

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