# High Risk Spyware

*Responding Safely to Targeted Surveillance*

High-risk spyware secretly monitors a device and can expose private communications, contacts, and location information. This guide is for suspected targeted surveillance, including risks to activists, journalists, dissidents, immigrants, and stalking victims. Prioritize physical safety, use a separate clean device, preserve evidence, and seek qualified help before attempting removal.

Common Signs of a Malware Infection:

- A trusted contact sends an unexpected installer, document, or download link
- Someone asks you to open a work-related file on your personal computer
- Someone offers unsolicited support or asks for remote access
- Private messages, contacts, or personal details are exposed or used in threats
- Unknown linked devices, login sessions, or account changes appear
- Unfamiliar programs start automatically or remote-control activity occurs
- Security protection is disabled or exclusions appear without explanation

These signs do not prove spyware or identify an attacker. A normal-looking device or clean antivirus scan does not rule out targeted compromise.

## Before You Begin – Important Warning

If anyone may be monitoring you, use a separate trusted device to seek help and plan changes with a safety advocate or qualified responder. Disconnecting, removing software, or changing accounts can alert the person monitoring you. Do not discuss safety plans near the suspected device. If you face immediate danger in the United States, call 911 from a safe phone.

Unplanned removal attempts can:

- Destroy messages, logs, or other evidence needed by investigators
- Reveal that you have discovered monitoring and increase retaliation risk
- Leave stolen account sessions or other compromised devices unaddressed
- Create false confidence while surveillance or account access continues

The September 15, 2026 UK–US–Netherlands advisory describes CHOSEN BRICK, Windows spyware linked to Iranian state cyber actors. Attackers build trust through WhatsApp, Telegram, or impersonation before sending convincing software or document lures. It steals communications, captures screens and audio, and survives reboot. Stolen information can create physical-safety risks. This guide also applies to other suspected targeted spyware; symptoms alone do not establish attribution.

# Malware Infection – Do This First

## Disconnect and Contain

Stop sensitive activity on the suspected device. A clean device is a separate trusted, updated device that has not opened the lure or granted the attacker access. Plan containment around safety and evidence preservation.

- Use a separate clean, updated device for help, recovery, and sensitive communication
- If safe, disconnect the suspected device from Wi-Fi, Ethernet, and Bluetooth
- Keep the suspected device away from:
- Private conversations and safety planning
- Clean devices, backups, and removable storage
- New passwords, recovery codes, and security-key setup
- Do not reboot, shut down, or reconnect solely to troubleshoot; ask a responder how to preserve its current state. Immediate physical safety takes priority.

## Preserve Evidence (If Needed)

For suspected targeted spyware, preserve evidence before cleanup whenever safe. Use the clean device to arrange secure collection with a responder.

- Record without reopening suspicious files:
    - Photos of visible alerts or suspicious messages, taken with a safe device
    - Sender usernames, profile links, phone numbers, and dates with time zones
    - Download links, filenames, and any requests to install software or grant access
    - Threats, exposed personal details, and suspicious account activity
- Write a timeline including:
    - When contact began and what the sender claimed
    - Which devices opened a file, installed software, or granted remote access
    - What accounts were used afterward and what changed
- Do not wipe, uninstall, delete logs, or publicly upload files or private messages. Keep originals where safe and ask a specialist how to transfer evidence securely.

## Decide: Self-Help or Expert Help

Choose qualified incident-response support immediately if:

- You suspect targeted surveillance, stalking, threats, or source exposure
- You opened the lure, installed its software, or granted remote access
- A provider sent a targeted-attack warning or you found unexplained sessions
- Your work, activism, family, or immigration context creates safety concerns
    - List personal and work devices for review, including borrowed or shared devices. Notify trusted workplace IT through a clean channel. Include phones and linked accounts; this does not mean CHOSEN BRICK infects every platform.

## Removing Malware (For Confident Users Only)

Targeted spyware requires expert-led handling, even for confident users. The steps below explain what to avoid until evidence and safety needs are assessed.

### Boot Into Safe Mode (If Possible)

For suspected targeted spyware, do not enter Safe Mode or restart as a self-help step. Rebooting can erase volatile evidence, and CHOSEN BRICK can survive reboot.

- Ask a responder whether forensic collection is needed before changing device state
- Follow their containment and examination instructions for each affected device

### Run Reputable Security Scans

A specialist should decide when scanning is safe and interpret the results. Antivirus alone cannot certify that targeted spyware is gone.

- Arrange checks of both personal and work devices, even if only one seems affected
- Have workplace IT or a qualified responder review persistence, security exclusions, logs, and indicators from the advisory
- Do not treat legitimate Telegram or cloud-service traffic alone as proof of infection
- Use only official vendor sources for security tools. Do not accept cleanup software, remote support, or downloads from the suspicious contact.

### Remove Suspicious Programs and Extensions

- Do not uninstall software or delete browser extensions before evidence collection
- Ask the responder to review startup entries, remote-access tools, browser extensions, and device-management settings
- Allow cleanup only after the responder has assessed evidence and safety needs

### Change Passwords (From a Clean Device)

Start account recovery on the clean device as soon as safely possible. Coordinate changes with a responder or safety advocate if they could trigger retaliation.

- Secure accounts in this order:
    - Primary email, recovery email, and password manager
    - Banking and other financial accounts
    - Messaging, cloud storage, and social media
    - Work or school accounts, together with trusted IT
- Use unique passwords; verify recovery addresses, phone numbers, and forwarding rules. Revoke unknown sessions, linked devices, app passwords, and connected apps. Enable phishing-resistant MFA, such as FIDO2 security keys or supported passkeys, on the clean device. Store backup codes safely. MFA does not remove spyware or invalidate every stolen session.

### If Removal Fails or You're Unsure

- Keep the suspected device isolated and use a clean replacement if necessary

- After evidence collection and with expert guidance:
  - Preserve necessary personal files separately; have a responder assess them before restoring. Do not restore unknown installers, programs, extensions, or a full compromised system image.
  - Have the responder determine whether a trusted OS reinstall or replacement is needed
  - Update the recovered device, enable protection, and restore only reviewed files
- Do not return to sensitive use until a qualified responder has assessed the device and account recovery. Reinstallation cannot undo information already stolen.

## Report the Incident (If Appropriate)

Suspected targeted compromise deserves reporting even without financial loss. Use a clean device and retain report numbers. Reporting does not replace urgent technical or safety support.

- FBI Internet Crime Complaint Center (IC3)
  - https://www.ic3.gov
  - Describe the contact, timeline, devices, suspected data theft, and any threats. For credible threats or suspected foreign-state targeting, also contact your local FBI field office through fbi.gov. IC3 is not an emergency service.
- Qualified incident-response support
  - Use a trusted provider experienced in targeted spyware and evidence preservation. For eligible activists, journalists, and civil society, Access Now offers free Digital Security Helpline assistance, subject to eligibility review.
  - https://www.accessnow.org/help/
- For stalking or partner abuse, consult a safety advocate using a safe device. Safety Net technology guidance: https://www.techsafety.org/technology-safety-quick-tips
- Geauga County
  - Contact local law enforcement about stalking, threats, or physical danger
    - https://www.geaugasheriff.org
  - Use 911 for immediate danger; use local non-emergency channels for other reports. Ask how to share evidence securely and avoid exposing sources or others in a public report.

## Recovery – After Malware Removal

- Continue safety planning; consider exposed contacts, sources, family, and locations
- Monitor logins, recovery changes, linked devices, forwarding rules, and financial activity
- With expert guidance, privately warn affected contacts through a verified safe channel. Stolen messages may be used to impersonate you.
- Reconnect only assessed devices. Follow up with the responder if warnings, threats, or unexplained access continue.

## How to Reduce Risk of Future Malware Infections

- Verify unexpected contact through a separate known channel before opening files
- Never move a suspicious work file to a personal device to bypass security controls
- Install from official vendor sites or app stores; keep OS and apps updated
- Keep antivirus and download warnings enabled; use phishing-resistant MFA where supported
- Limit public personal details and create a trusted escalation plan before an incident