THE CISO PERSPECTIVE

TECH INSIGHT. NO HYPE.

VIDEO CHEAT SHEET

What is ClickFix?

Fake CAPTCHA Attacks Explained

cisoperspective.com

Watch the video

TL;DR

ClickFix is a social engineering technique that tricks users into running a malicious command themselves. A fake CAPTCHA or error page copies a hidden command to the clipboard, then walks the victim through Win+R, Ctrl+V and Enter. No software exploit is required: the user's own click becomes the initial access.

47%

of initial-access attacks in Defender Experts notifications were ClickFix, ahead of phishing at 35%

Microsoft Digital Defense Report · 2025

563%

year-over-year rise in fake CAPTCHA lure incidents in 2025

CrowdStrike Global Threat Report · 2026

1.6M+

fake CAPTCHA detections ESET blocked in just six months (H1 2025)

ESET Threat Report · H1 2025

THE ATTACK FLOW

Five steps, one user action. Each stage is a chance to break the chain.



01 Fake CAPTCHA — Lure page asks the user to "verify you are human"

02 Clipboard copy — Page JavaScript silently writes a command to the clipboard

03 Win+R → paste — Victim is told to press Win+R, Ctrl+V, Enter

04 PowerShell — Hidden window pulls the next stage from the web

05 Payload — Infostealer, RAT, sold access or ransomware

LURE | USER-ASSISTED EXECUTION | LIVING OFF THE LAND | IMPACT

KEY TERMS

ClickFix	Social engineering that tricks a user into pasting and running a malicious command.
MITRE T1204.004	MITRE ATT&CK: User Execution — Malicious Copy and Paste.
ConsentFix	Variant that steals an OAuth consent / auth code instead of installing malware.
FileFix	Variant that has the user paste into the File Explorer address bar.
Infostealer	Malware that harvests passwords, cookies and session tokens (e.g. Lumma, Vidar).
ASR rules	Attack Surface Reduction policies that block risky script and LOLBin behavior.

DEFENSE CHECKLIST

For users

- [x] A real site never asks you to press Win+R or open a terminal
- [x] Never paste a command a web page "copied for you"
- [x] Close the tab and report the page to security
- [x] If you already ran it: disconnect and call the help desk

For security teams

- [x] Cut delivery: DNS/web filtering, ad blocking, SmartScreen
- [x] Browser/clipboard: Chrome Enhanced Protection; screen clipboard copies
- [x] Restrict the Run dialog and limit local admin rights
- [x] Block execution: app control, PowerShell limits, ASR rules
- [x] Detect and respond with EDR; revoke stolen sessions and tokens

CISO TAKEAWAY

Because ClickFix has multiple stages, no single control stops it. Build multiple chances to interrupt the chain — and remember: a legitimate website will never ask you to paste and run a command.

JUMP TO A CHAPTER

each one opens the video at that moment

- 0:00 Why ClickFix matters
- 1:10 What is ClickFix?
- 2:57 How the attack works
- 4:10 What attackers do next
- 5:18 Defense: breaking the chain
- 7:22 Wrap-up

TCP MEDIA

© 2026 TCP Media · Free to share with attribution · @cisoperspective