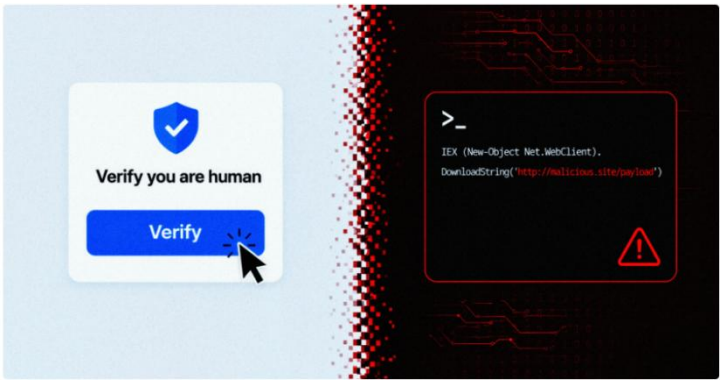
ClickFix: When “Fix It” Is the Trap



ClickFix turns a fake problem into a real compromise

ClickFix is a social engineering attack that tricks people into running malicious commands on their own devices. Instead of sending an obvious attachment or asking for a password, the attacker shows a fake error message, fake CAPTCHA, fake browser update, fake meeting issue, fake file problem, or fake “security fix.” The page then tells the user to copy and paste a command into Windows Run, Windows Terminal, PowerShell, Command Prompt, File Explorer, or macOS Terminal.

Why this matters

- **It bypasses normal instincts:** The user may think they are fixing a small technical issue, proving they are human, opening a document, joining a meeting, or installing a trusted update.
- **It uses trusted tools:** The command may run through built-in tools such as PowerShell, Windows Run, Terminal, mshta.exe, wscript.exe, or other legitimate utilities.
- **It can get past some security controls:** Because the user launches the command, the attack may avoid some traditional email, web, and download protections.
- **It can lead to serious impact:** Reported ClickFix payloads include credential stealers, remote access trojans, loaders, backdoors, and ransomware-related tools.

What it may look like

- **Fake verification:** “I’m not a robot,” “Verify you are human,” or “Complete the security check.”
- **Fake document issue:** “The file cannot be displayed,” “Document viewer failed,” or “PDF download interrupted.”
- **Fake browser or software update:** “Chrome/Edge needs a security update,” “Install this codec,” or “Update required to continue.”
- **Fake work process:** “Join this Teams/Zoom/Webex meeting,” “Complete compliance training,” “Set up this AI tool,” or “Authorize this app.”

How ClickFix attacks work

1. **The lure** - The user lands on a page through phishing, malvertising, a search result, a QR code, or a compromised website.

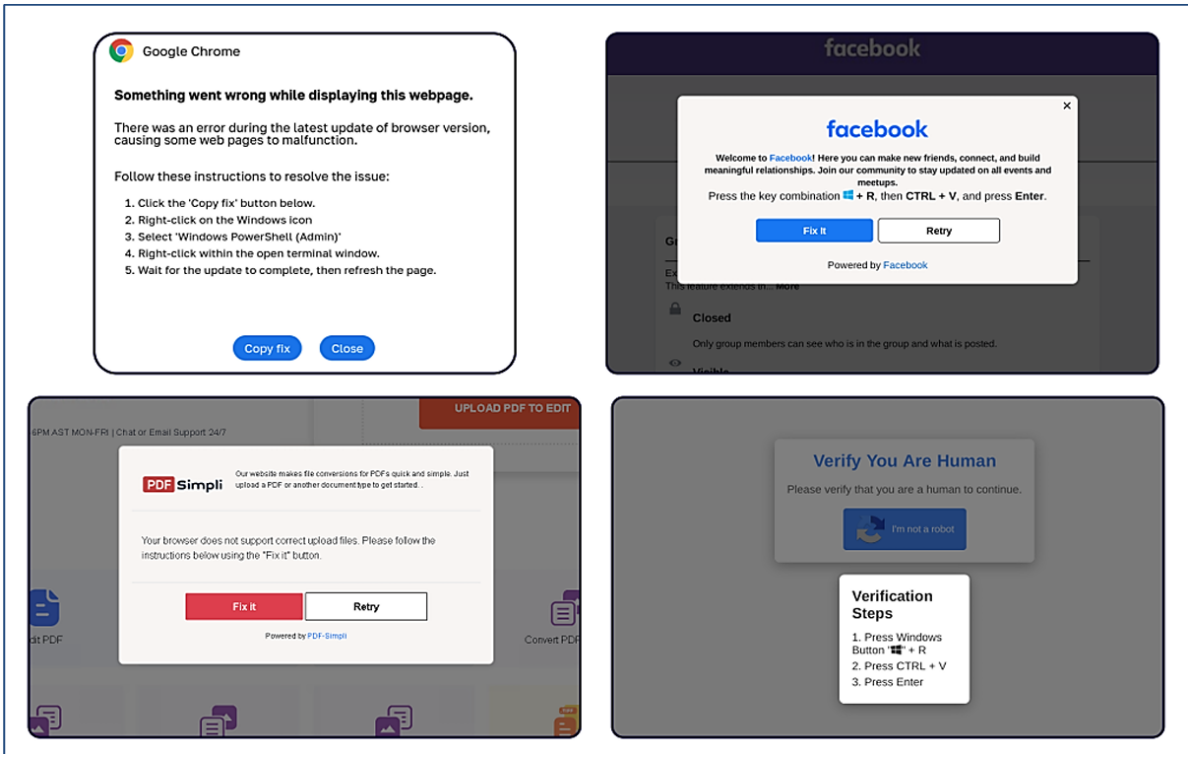
2. **The fake problem** - The page creates urgency with a fake technical issue, CAPTCHA, document error, browser crash, update prompt, or business-process request.

3. **The clipboard or repair trick** - The site may copy a command to the clipboard, tell the user exactly what keys to press, or provide a fake repair file/tool.

4. **User-level execution** - The user is instructed to paste and run the command in Windows Run, Terminal, PowerShell, File Explorer, or macOS Terminal.

5. **Follow-on compromise** - The command downloads malware, opens remote access, steals credentials/session data, or installs persistence.

Featured below are some examples of malicious websites that impersonate Google Chrome, Facebook, PDFSimpli, and reCAPTCHA using the ClickFix social engineering tactic.



Common variants now being reported

- **Classic ClickFix:** The user is asked to press Win+R, paste a copied command, and press Enter.
- **FileFix:** The user is told to paste into the File Explorer address bar instead of the Run dialog.
- **TerminalFix:** The user is told to open PowerShell or Terminal and paste a command directly.
- **DownloadFix:** A fake failed download offers a “repair tool” or script to fix the problem.
- **CrashFix:** A malicious browser extension or page deliberately creates browser problems, then presents a fake recovery/security prompt.
- **ConsentFix:** Instead of running a command, the user is tricked into approving a malicious OAuth app with broad access.

How to spot a ClickFix attack

A quick self-check before clicking “fix”

Ask yourself:

- Did a website tell me to run a command? Stop. Close the page and report it.
- Did the command come from a random page, ad, email, or QR code? Do not run it.
- Am I being asked to install a browser extension or update from a pop-up? Go to the official vendor site or ask ITS if at work.
- Am I being asked to grant broad account permissions? If at work, verify with Metro ITS before approving. If at home, look for tech support on the site in question.

Red flags

- **A website asks you to press** Win+R, Win+X, Ctrl+V, Enter, or other keyboard shortcuts to “fix” something.
- **A browser page tells you to open** PowerShell, Terminal, Command Prompt, Windows Run, or File Explorer and paste text.
- **A page says a** document, invoice, shared file, meeting, update, CAPTCHA, printer, or AI tool will not work unless you run a command.
- **A “verification” step copies something** to your clipboard or gives instructions that feel more like IT troubleshooting than normal login.
- **A link came from an unexpected email**, text, QR code, ad, search result, social post, or external website.
- **The page uses urgency:** “required,” “blocked,” “security update,” “session expired,” “complete now,” or “fix immediately.”

What should you do

- **Do not paste commands from a website.** Never copy/paste text from a browser into Windows Run, PowerShell, Terminal, Command Prompt, File Explorer, or macOS Terminal unless ITS specifically directed you to do so through a trusted support channel. If you are at home, then reach out to tech support for the site.
- **Stop if the page provides step-by-step keyboard instructions.** Real CAPTCHA checks and normal website errors do not require you to run system commands.
- **Use trusted navigation.** For Metro systems, use a saved bookmark, a known Nashville.gov or Metro URL, or an approved application shortcut instead of following unexpected links. At home, use a web browser to search for the legitimate site.
- **Be cautious with “helpful” fixes.** Attackers count on people wanting to solve the problem themselves. It is safer to pause and report than to troubleshoot a suspicious prompt.
- **Do not approve unexpected app permissions.** Treat consent screens, “connect account” prompts, and broad permission requests as high risk unless expected and approved.
- **Report it quickly.** If you see a ClickFix-style prompt or already ran a command at work, contact the Metro ITS Help Desk immediately.

Key takeaway

Do not let a website become your IT support technician. A real website should not need you to paste commands into system tools. When a prompt tells you to “fix” a problem by running a command, stop and report it.

Additional Resources

- Microsoft Security Blog: Think before you Click(Fix)
- HHS HC3 Sector Alert: ClickFix Attacks
- Huntress: ClickFix Attack Variants, Detection & How It Works
- revel8: ClickFix Attacks in 2026
- Cybersecurity News: What is ClickFix Attack
- The Hacker News: ClickFix Campaigns Expand Malware Delivery

---