



The Fake Fix

What Is a ClickFix Scam?

Keeping your software up to date helps close security gaps. But attackers can turn that good habit, and your instinct to solve a problem quickly, against you.

The technique is called **ClickFix**. It is a social engineering attack that tricks you into copying and running a malicious command. Instead of forcing their way into your system, attackers persuade you to open the door yourself.¹

The attack may begin with a phishing message, compromised website, fake CAPTCHA, or pop-up claiming that something is wrong with your device. It may use specific details to sound convincing: "Warning! A security scan found **47 threats** on your computer."

Then it offers a **"fix."** You may be told to open Windows Run, PowerShell, Command Prompt, or Terminal, paste a command, and press Enter.

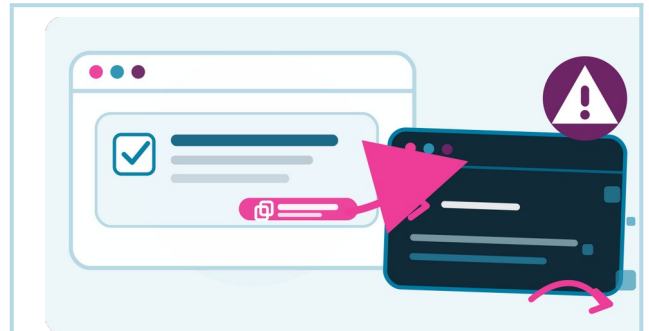
That command can **install malware, steal passwords and files**, or give an attacker **remote access**.

ClickFix is especially dangerous because the harmful action is initiated by the user. That can help the attack slip past some conventional filters and security checks, particularly when the command uses legitimate tools already installed on the device.

Already followed the instructions? Stop and contact your IT or security team immediately.

Remember this rule: A legitimate CAPTCHA, error message, update prompt, or software download will not ask you to paste a command into Windows Run or a terminal.²

Close the message and update through your device settings, the app's built-in updater, or an official support page you navigate to independently.



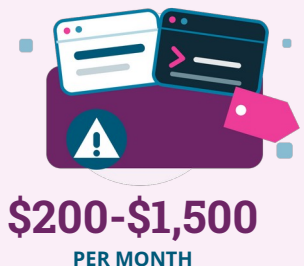
Five Signs the "Fix" Is Fake

ClickFix lures mix familiar branding with pressure and technical-sounding instructions. Stop when you see these signs:

- 1 It impersonates a trusted brand, verification service, or support provider.
- 2 It names a specific threat or an alarming number of infections.
- 3 It uses a countdown timer or pressures you to act immediately.
- 4 It tells you to open Windows Run, PowerShell, Command Prompt, or Terminal.
- 5 It asks you to paste a command or disable your firewall, antivirus, or another security feature.

Scams for Sale

Microsoft Threat Intelligence has found **ClickFix builders** advertised on hacker forums. These kits can generate fake landing pages, create malicious commands, and imitate familiar services such as **Cloudflare**. Subscriptions have been advertised for between **\$200 and \$1,500 per month**, while individual components have been offered for **\$200 to \$500**. By packaging the lure, instructions, and technical setup together, these services make it easier for less-skilled criminals to launch their own attacks.¹



1. Microsoft: Think before you Click(Fix)
2. Microsoft: How a macOS ClickFix campaign learned to hide