Meta Keywords: **what is ClickFix, ClickFix attack, ClickFix malware, ClickFix fake CAPTCHA, ClickFix cybersecurity, ClickFix social engineering, how does ClickFix work, how to protect against ClickFix, how to detect ClickFix attacks, how to identify a ClickFix scam, how to know if a CAPTCHA is fake.**

Topic: What Is ClickFix? How Fake CAPTCHA Scams Install Malware

Slug: https://lomatechnology.com/blogs/what-is-clickfix-fake-captcha-malware

Meta Descriptions: **What is ClickFix? Learn how fake CAPTCHA scams trick users into running malicious commands and exposing sensitive information.**

The tricks cybercriminals use to get people to install malware are always changing. People who are targeted by traditional attacks usually do something bad, like download an unknown document, open a file that is infected or click on a clearly harmful link. But a newer method is different: attackers don't sneakily use the computer to do bad things; instead, they convince the victim to do the wrong thing themselves. This method is called ClickFix.

So, what is ClickFix? As part of ClickFix, attackers make a fake error message, fake CAPTCHA, fake browser notification or fake security verification page. They then try to trick users into following the instructions, which run a malicious command. The victim usually thinks they are just proving they are human, fixing a browser issue or going through a normal verification process, so the attack looks harmless.

Microsoft calls ClickFix more of a complex social engineering method than just a family of malware. Fake CAPTCHAs or error messages can be used in this method. These can copy a malicious command to the clipboard and tell the user to paste it into Windows Run, Windows Terminal or another system utility.

The target might not know they are running code, which is a risk. "Check that you are human" "Fix your browser" or "Press Windows + R and paste the verification code" are some of the things that a page might say. If you are used to seeing CAPTCHA challenges online the steps might look like they are real.

This is why what is ClickFix is an increasingly important question for employees, Website viewers, IT teams and regular people who use the internet. The method does not only rely on program vulnerabilities; it also targets how people act.

Security experts have seen ClickFix campaigns send loaders, information thieves, remote-access trojans and other harmful software. Malware like Lumma Stealer,

XWorm, VenomRAT, AsyncRAT, Danabot and NetSupport RAT have been used in operations that Microsoft knows about.

The method has also been used on platforms other than Windows. In August 2026, Microsoft said that campaigns like ClickFix that target macOS can get people to copy and run commands in Terminal by showing them fake verification or download pages.

This means that ClickFix is not just another fake CAPTCHA. As part of a larger shift in social engineering, attackers are now making websites that make people want to be involved in the process of spreading software.

What Is ClickFix? Understanding the ClickFix Attack

To answer what is ClickFix, it helps to tell the method apart from the malware it might install. ClickFix is a way to trick people into giving you money, not a specific piece of malware. Attackers trick people into running a command that downloads or starts malware by showing them fake errors, CAPTCHAs or security checks also.

A typical ClickFix chain is: Malicious link or website → Fake prompt → User interaction → Malicious command → Malware download → Infection

How does ClickFix work?

Step 1: The victim reaches a malicious page

The victims may get there by: an email scam, not a good advertisement, a website that was hacked, a fake file or download of software, a message on social media, a result from a search engine and an HTML file that is harmful.

The page might pretend to be a well-known brand, government service, tourist website, or tech company. Microsoft has seen campaigns that use fake ClickFix CAPTCHA prompts to look like they are from Booking.com.

Step 2: A fake problem appears

The website shows a problem that supposedly needs to be fixed right away, like: "Prove that you are a person." "Your browser needs to be checked." "This page won't load right."

"To go on, press Windows + R." "Make a copy of the command to verify."

This is where ClickFix social engineering becomes effective also. The victim believes they are fixing a minor issue rather than installing malware.

Step 3: The user copies and executes a command

The page might copy an order to the clipboard and tell the victim to: press a key combination, startup PowerShell, Windows Run, or Terminal, paste the order and type "Enter." ClickFix campaigns may use legal tools like PowerShell, mshta.exe, and curl in bad ways to download or run extra material.

Step 4: The command downloads malware

The order could get malware from a server that an attacker controls. Some possible results are: theft of passwords and browser cookies, theft of money or cryptocurrency, logging keys, access from afar, more installation of malware and getting data stolen.

Depending on the strategy, the same ClickFix page could send out different malware.

Why is ClickFix effective?

ClickFix makes it look like a regular user action when malware is being run. Even if security software finds a suspicious download, the victim is still tricked into running a real system utility and carrying out the malicious command. PowerShell or Windows Run are not always the danger. The command that the user was convinced to run is the threat.

Microsoft has reported ClickFix activity affecting thousands of enterprise and end-user devices globally. This is why what is ClickFix has become an important cybersecurity question for individuals and organizations.

ClickFix Fake CAPTCHA: How “I’m Not a Robot” Becomes a Malware Trap

One of the most common ClickFix variants uses a fake CAPTCHA. CAPTCHAs are well-known ways to tell the difference between people and bots, which makes them easy for attackers to copy also. A fake CAPTCHA doesn't have to be perfect; it just needs to look real enough to get people to do dangerous things.

1. How to know if a CAPTCHA is fake: You shouldn't have to open Windows Run, PowerShell, Terminal, or another command-line tool and run a command in order to solve a real CAPTCHA. You should never have to run a command on your computer to solve a CAPTCHA. Stop right away if a CAPTCHA tells you to press Windows + R, write text, open PowerShell or Terminal or do anything else that isn't in the browser.

2. Common signs of a fake CAPTCHA: Keep an eye out for these signs: The CAPTCHA shows up out of the blue. The domain looks like it's not familiar or is wrong. The page uses threats or sense of urgency. To do this, press Win + R. You need to copy and paste something into Run. The page will copy text to your clipboard for you. A "verification code" is what the command is called. The site pretends to be a reputable

business. You get a strange file or script. There are strange words or mistakes on the page.

Example 1: Fake Booking website

Microsoft found evidence of a phishing campaign that pretends to be Booking.com. Attackers sent hotel companies to fake Booking.com pages with CAPTCHAs on them. People were told to copy and paste a code into Windows Run and run it.

Malware like XWorm, Lumma Stealer, VenomRAT, AsyncRAT, Danabot and NetSupport RAT were sent out as part of the effort. The most important thing to learn is that a website that looks professional does not mean that it is real.

Example 2: Fake Cloudflare verification

Hackers have also made ClickFix pages that look like Cloudflare Turnstile. Websites that had been hacked showed fake pages for human verification that led users to run malicious commands. This shows why people shouldn't trust a security message just because of how it looks.

Why fake CAPTCHA attacks work

These con games use:

- Being familiar: People are used to seeing CAPTCHA interfaces and may trust them without thinking about it.

- The Power: A security prompt looks official and keeps you safe also.

- Hurry up: Attackers might say that the browser won't work until proof is done.

- Easy Living: Users might think that hitting a few keys won't hurt them.

- Behaviors for fixing problems: ClickFix tells people to fix problems right away without thinking about what the rules say.

This is the core of ClickFix cybersecurity risk: attackers manipulate users instead of relying only on software vulnerabilities.

The most important CAPTCHA rule

When asking how to know if a CAPTCHA is fake, remember:

If it asks you to execute a command outside the browser, do not do it. Close the page, don't run copied content and use a reliable source to check the website.

ClickFix Malware and ClickFix Social Engineering: What Happens After the User Clicks?

Understanding what is ClickFix malware means recognizing that ClickFix is usually a delivery method, not a specific malware family. Attackers can use the same method to send loaders, information thieves, remote-access trojans, banking malware, password thieves and other harmful programs.

1. ClickFix attack chain: A typical ClickFix attack follows these stages:

Stage 1: Initial lure

What attackers do: phishing, putting up ads, websites are at risk, not real papers, links to social networks the search results and redirects with bad intent.

Stage 2: Fake verification

Attackers use phishing emails, ads with malicious code, websites that have been hacked, fake documents, social media links, search results and malicious redirects to get people to a fake page.

Stage 2: Fake verification

The victim sees a fake CAPTCHA, browser error, security alert, download problem, software update, account verification request or “human check.”

Stage 3: Command preparation

The webpage may copy malicious content to the clipboard or instruct the user to copy it manually.

Stage 4: User execution

The victim is told to open Windows Run, PowerShell, Windows Terminal, Command Prompt or macOS Terminal and paste or enter the provided command.

Stage 5: Payload delivery

The command contacts an external server and downloads additional code.

Stage 6: Malware execution

The final payload may steal information, provide remote access, or install more malware.

This explains why ClickFix social engineering is so effective: the user becomes the link between the malicious webpage and the operating system.

What types of Malware can ClickFix deliver?

ClickFix ads could bring you: theft of information, trojans for remote access, Malware for banks, thieves of credentials, lifters, RATs and tools for watching your screen.

Microsoft has heard of ads using Lumma Stealer and other malware that steals credentials. Browser passwords and cookies can be stolen by hackers, and remote-access trojans can let attackers take control of the device.

How to detect ClickFix attacks

Keep an eye out for these signs:

It says on the page to open Run or Terminal.

For a CAPTCHA, you have to copy and paste a code.

A website changes your clipboard without telling you.

After going to a sketchy page, PowerShell opens.

After that, a strange program shows up.

Your browser is acting strangely.

An warning is made by security software.

IT departments should look into PowerShell, mshta, rundll32, wscript, curl and wget usage that doesn't seem right. Other signs are URLs that look fishy, direct IP addresses, shortened links, strange domains and scripts or files that you wouldn't normally find.

Evidence Guide for security teams

Possible evidence includes browsing history that shows odd behavior, malicious redirects, newly visited domains, or fake CAPTCHA pages. Endpoint proof could include Run dialogs, suspicious scripts, unexpected child processes or other strange command-line behavior. Connections to domains you aren't familiar with, direct IP connections, or downloads that happen right after a command is run can all be examples of network evidence. Unusual scripts, archives, executables, deceptive file extensions or new temporary files may be found in file evidence. Additionally, user reports can be very helpful, especially when they show fake CAPTCHAs, browser "repair" directions or strange command-line windows.

Multiple signs should be compared by security teams instead of viewing a single suspicious event as proof of an infection.

How to Identify a ClickFix Scam and How to Protect Against ClickFix

Knowing how to identify a ClickFix scam matters because the victim often has to help with these attacks. ClickFix lets users stop the infection, unlike automatic exploits.

1. A CAPTCHA asks you to use Windows Run: A legitimate CAPTCHA should not require: Win + R → Paste → Enter

If a webpage gives these instructions, close it immediately.

2. A website asks you to open PowerShell: PowerShell is a legitimate administration tool, but ordinary websites should never ask visitors to open it and run commands.

3. The command is called a verification code: Attackers may describe malicious commands as: verification codes, security commands, browser repair commands, CAPTCHA codes and update commands.

4. The label does not make the command safe: Your clipboard changes unexpectedly. If a website copies text you did not intentionally select, do not paste or execute it.

5. The domain looks wrong: Attackers often imitate trusted brands while using unrelated domains. Always check the full website address.

6. The page creates urgency: Warning signs include: “Your browser is infected.” “Verification required immediately.” “Your session will expire.” “Click now to continue.” “Security verification failed.” Urgency is a common social engineering tactic.

7. How to protect against ClickFix: A strong how to protect against what is ClickFix strategy combines awareness, security tools and safe online habits.

For individual users: never execute commands provided by unfamiliar websites, do not paste unknown text into PowerShell or Terminal, treat unexpected CAPTCHA instructions as suspicious, check website domains carefully, avoid suspicious email links and downloads, keep your browser and operating system updated, use reputable security software, enable multifactor authentication, close suspicious browser tabs, stop if a website asks you to perform an unusual action.

For organizations: Companies should use: security awareness training, phishing simulations, endpoint detection and response, web and email filtering, powerShell and script monitoring, network monitoring, browser protection, least-privilege access and incident-response procedures.

Because the user initiates execution, ClickFix can bypass some traditional security assumptions. Monitoring suspicious domains, command-line tools and unusual script activity can help detect these attacks.

What to do if you already executed the command

Should you think you have a ClickFix infection:

If necessary, take the device off of the internet.

Don't connect with the sketchy page anymore.

If it is a work gadget, call your IT or security team.

Use reliable tools to do a full security scan.

Use a clean device to change your important passwords.

Watch your account behavior for logins that don't seem right.

If sensitive information could be exposed, keep an eye on your bank accounts.

Keep track of URLs, emails, screenshots, alerts and other proof.

Malware may leave behind extra files, so it's important to keep security standards up to date and do a full scan.

A simple rule for employees: Websites should never tell you to run commands on your computer.

By following this rule, you can stop many ClickFix attacks without needing to know a lot about computers.

ClickFix Cybersecurity: Why This Threat Matters in 2026

The importance of ClickFix cybersecurity comes from the technique's adaptability. With the same social engineering method, attackers can change the fake question, impersonated brand, delivery method or malware. In March 2026, Microsoft said that CAPTCHA-gated phishing more than doubled, with 11.9 million attacks. This was the highest monthly volume seen in the previous year. This rise shows why being aware is still important.

1. ClickFix Is Becoming a Cross-Platform Problem: A lot of the first what is ClickFix efforts were aimed at Windows using tools like PowerShell and Windows Run. Attackers have, however, changed the method to work on macOS as well. Microsoft kept track of an effort in August 2026 that got people to copy and run commands in Terminal. Because of this, ClickFix is not just a Windows threat.

2. Attackers Can Imitate Trusted Brands: Fake pages might look like: cloud flare from Google, websites for booking, help from the government, social networking sites, services from Microsoft, platforms for streaming and websites where you can get software.

A well-known logo or a skilled design doesn't mean the product is real. HTTPS only makes the connection safe; it doesn't prove that the website is real

3. ClickFix Attacks Exploit Trust: In traditional hacking training, files and attachments that look fishy are often the main focus. One more important lesson is added by ClickFix:

It's not enough to trust instructions just because they're on a website.

Watch out if a page: looks professional, but the domain is one I'm not familiar with, shows an unexpected CAPTCHA, it tells you to start Command Prompt, Run, PowerShell or Terminal, text is copied automatically to your clipboard, uses fear or hurry and says it needs a security command.

4. A Practical Decision Framework: When a webpage asks you to take an unusual action, ask:

- Did I intentionally visit this website? If not, be cautious.

- Is the domain exactly what I expected? If not, stop.

- Is the website asking me to leave the browser? Never open a system tool or execute a command because a webpage tells you to.

- Is it asking me to paste something I did not create? Do not execute unknown commands.

- Is the page using urgency or fear? Attackers use pressure to discourage careful thinking.

- Can I complete the task through the official website or application? If so, close the suspicious page and navigate directly to the legitimate service.

Evidence Guide: Investigating a Suspected ClickFix Incident

If an organization suspects a ClickFix attack, investigators should collect evidence systematically.

1. Identify the entry point: Check to see if the person received: a message or link, an HTML file attachment, not a good advertisement, a website that was hacked and a fake page to download also.

2. Preserve website evidence: Record the: full URL and domain, timestamp, referring page, Email source and browser history.

3. Review endpoint activity: Look for unusual execution involving: PowerShell, Command Prompt, Windows Run, mshta.exe, rundll32.exe, wscript.exe, curl.exe, wget.exe. These tools can provide useful indicators during a ClickFix investigation.

4. Check behavior on the network and in files: Check out the links that were made after the command was run and look for scripts, archives, executables or other files that seem odd also.

5. Look at the display of credentials: If you think someone stole your information, look into the credentials that were saved or entered on the device.

6. Keep it in check and fix it: Follow the steps for responding to an event to separate the device, get rid of any malicious software, reset the credentials, check for persistence and keep an eye on any connected systems.

Conclusion

So, what is ClickFix? ClickFix is a form of social engineering that gets people to run malicious orders that look like CAPTCHA checks, browser fixes, software updates or security checks.

Attackers don't use a technology flaw to their advantage; instead, they convince their victims to do something dangerous on their own.

Someone could start Windows Run, PowerShell, Windows Terminal or macOS Terminal because a website says they need to. After that, the command can download malware, steal login information, or let attackers get in remotely.

The main lesson is that you shouldn't always trust security prompts that look like they know what they're doing. Browser warnings, proof pages and CAPTCHAs that aren't real can look a lot like real ones.

To stay safe, never run commands from websites you don't know or put text from websites you don't know into PowerShell, Terminal or Windows Run. A real CAPTCHA shouldn't need to be run from the command line. Always check the website domain, be careful when the clipboard changes without warning and don't rush because of urgent alerts.

Companies should teach their workers that harmful directions can show up on websites too, not just in questionable emails or attachments.

The key principle behind how to protect against ClickFix is simple: never execute a command merely because a website tells you to do so. When in doubt, close the page, visit the official website directly and verify the request through a trusted channel.