Willow Valley Computer Club

Member of apcug

An International Association of Technology & Computer User Groups

The Fix Is In

How Scammers Trick You Into Hacking Yourself

Al Williams

May 7, 2026

A new family of cyberattacks is tricking people into hacking themselves.

The siblings are called ClickFix, FileFix, and ConsentFix.
And the list of siblings is growing

The Scale of the Problem

ClickFix attacks surged 517% in the first half of 2025, making them the #2 attack method globally, behind only phishing.

FileFix, a variant of ClickFix, was discovered in June 2025. Within two weeks, threat actors were testing it in real attacks.

ConsentFix, discovered in December 2025, can take over your Microsoft account without ever stealing your password or triggering multi-factor authentication.

These attacks are used by criminal gangs and nation-state hackers from Russia, North Korea, and Iran.

Source: ESET H1 2025 Threat Report; Push Security Research, December 2025; Check Point Research, July 2025

What All "Fix" Attacks Have in Common

In every case, you do the attacking for the criminal.

1. Bait — You visit a webpage that shows a fake error, CAPTCHA, or file-sharing notice.

2. Copy — The page secretly places a malicious command or URL on your clipboard.

3. Paste — You are told to paste something into your computer to "fix" or "verify" the issue.

4. Damage — The pasted content runs malware, steals information, or hijacks your account.

Because you perform the action yourself, your antivirus and security software often can't stop it.

ClickFix — The Original "Copy-Paste" Attack

- You visit a website that shows a fake error, browser update, or CAPTCHA puzzle.
- A button says "Fix It" or "Verify." Clicking it secretly copies a dangerous command to your clipboard.
- You are told to press Win+R to open the Run dialog box and paste the command.
- Pressing Enter runs the hidden script, which installs malware — software that steals your passwords, credit card numbers, and personal information.
- First seen in early 2024. Surged 517% in 2025.
- Works on Windows, Mac, and Linux.
- Apple added a new macOS Terminal warning specifically to counter ClickFix.

Source: Proofpoint, March 2024; ESET H1 2025 Threat Report; Microsoft Security Blog, August 2025; Sophos, March 2026

ClickFix — What It Looks Like

You might see a fake CAPTCHA that says:

```
Verify you are human
1. Press  Win + R
2. Press  Ctrl + V
3. Press  Enter
```

Or a fake error message that says:

"Your browser is out of date. Copy and run this fix to continue."

No legitimate website will ever ask you to do this

FileFix — Same Trick, Friendlier Disguise

FileFix is a variant of ClickFix discovered by security researcher mr.d0x in June 2025.

Instead of asking you to open the Run dialog box (which looks suspicious), FileFix uses something much more familiar: the Windows File Explorer address bar.

A fake page says a file has been shared with you. You click "Open File Explorer" — a real File Explorer window opens.

A hidden command is placed on your clipboard. You're told to paste a "file path" into the File Explorer address bar.

What looks like a file path is actually a long-hidden command. Spaces push the real command out of view. Pressing Enter runs the malware.

File Explorer feels safe and ordinary. Most people don't know it can run commands.

Source: BleepingComputer, June 2025; Check Point Research, July 2025; Kaspersky, November 2025

ConsentFix — The Most Sophisticated Variant

1. You find a website through Google Search. The site has been compromised by hackers.

2. A fake Cloudflare verification asks for your business email address.

3. A "Sign In" button opens a real Microsoft login page. If you're already signed in, you just click your name.

4. Microsoft redirects you to a page with a special URL. You're told to paste that URL back into the original site.

5. That URL contains an access token. The attacker now controls your Microsoft account.

No password is stolen. No MFA is triggered. Even passkeys don't help.
The attack happens entirely inside your browser.

Note: The campaign discovered so far targets business/organizational Microsoft accounts, not personal Outlook or Hotmail accounts. The social engineering pattern could be adapted to other services.

The "Fix" Family at a Glance

	ClickFix	FileFix	ConsentFix
First Seen	Early 2024	June 2025	December 2025
Bait	Fake CAPTCHA or error message	Fake file-sharing notice	Fake Cloudflare verification
Where You Paste	Run dialog (Win+R)	File Explorer address bar	Back into the phishing page
What Happens	Malware installed on your computer	Malware installed on your computer	Microsoft account hijacked
Bypasses MFA?	N/A (installs malware)	N/A (installs malware)	**Yes — even passkeys**

How to Protect Yourself

- Never paste commands from a website into your computer

No legitimate site will ever ask you to open the Run box, Terminal, or paste into File Explorer.

- Treat "fix it" prompts as red flags

Fake CAPTCHAs, error messages, and "verification" steps are the #1 lure.

- Never paste URLs to "verify" your identity

Real login pages don't ask you to copy URLs between pages.

- Contact the Computer Club if something seems off

We would rather check a false alarm than clean up after an attack.

If a website's instructions ask you to do something outside of the browser – that is a red flag! Don't do it!

If a website tells you to
copy, paste, or run anything
on your computer, including macOS

stop.

Close the page.
Contact the Computer Club.
You are always better off asking than acting.

Don’t click on links in emails

stop.

Delete the email.
If you clicked the link, contact the Computer Club.

For In-Home Help

GetHelp@WVComputerClub.org

or

717-464-6330, Option 1

For Technology Center walk-in help

North, J Building, 5th Floor
Thursdays, 10 am to 4 pm

or

717-464-6330, Option 2

Questions?