# Clickfix scam: How this attack works and how to protect yourself

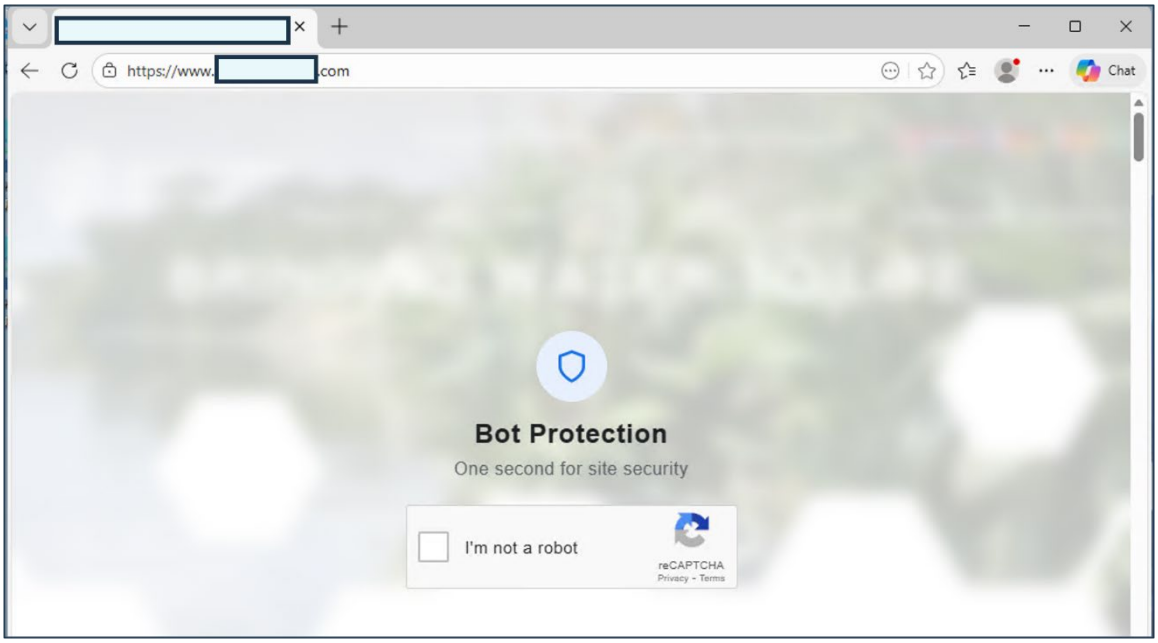
## What is ClickFix?

ClickFix is an attack technique we have now observed in four separate client incidents within the last two weeks. It uses a manipulated website to trick users into executing malicious code directly on their own device

**This real-life example demonstrates how easily a trusted website can be compromised.**

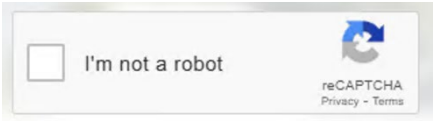
## How did the website become a risk?

The client visited this vendor's website regularly and trusted it, which meant their guard was naturally down. However, unknown to them, the website had been compromised.



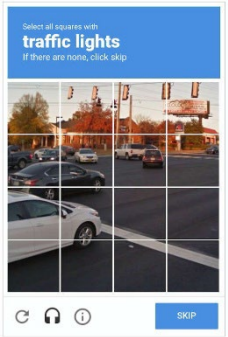

## What does the user see first?

One day, the user visits the same trusted website and is presented with a CAPTCHA. This is not unusual, so there is no immediate reason for suspicion. They click the "I'm not a robot" checkbox.



Under normal circumstances, the CAPTCHA would either:

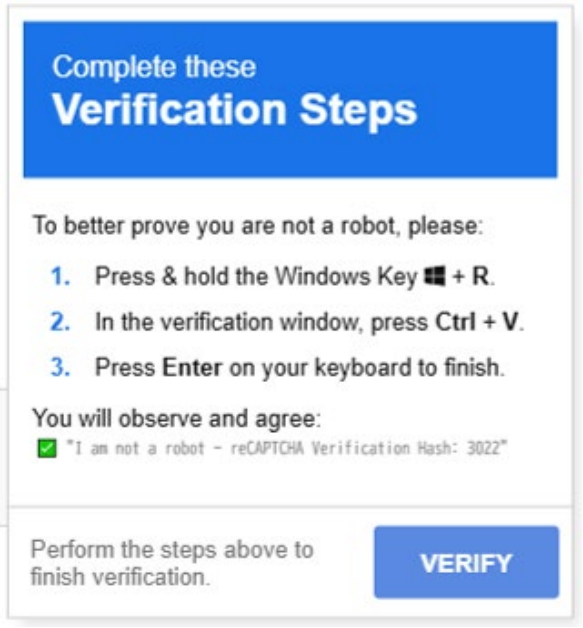
- load the page, or
- present the familiar “select the traffic lights/motorbikes” verification step.




## What happens instead?

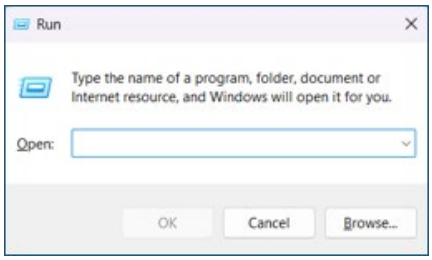
Rather than proceeding, a **pop-up appears**, instructing the user to press **Windows + r**.

## This is the moment the scam begins.




The Windows + r shortcut opens the **run** dialog on a Windows device, a system-level tool used to execute commands. **A legitimate website would never require this.**

## What happens if you click Windows + r?




If the user follows the instruction and presses **Windows + r**, the attacker gains the opportunity to run commands on the device. The user is then prompted to press **ctrl + v**, which pastes malicious code that was silently copied to the clipboard. When the user presses **enter**, that code:

- Downloads a malicious executable, and
- Installs it directly on the device.

## From this moment, the device is compromised.

## What can the attacker do next?

Once the malicious code runs, the attacker may:

- Steal active Microsoft login sessions (giving them access to email)
- Steal browser credentials (giving access to other applications)
- Execute further malicious code
- Install a remote access tool (gaining persistent control of the device)

These actions can bypass a wide range of standard organisational security controls.

## Why does this attack work?

Cybercriminals continually experiment with new techniques to avoid detection and circumvent preventative measures. This attack is effective because:

- It relies on *trusted*, familiar websites.
- It uses system shortcuts many users do not understand.
- It imitates a legitimate captcha flow.
- It leverages user behaviour rather than software vulnerabilities.

This does not mean existing security controls are ineffective, but it **does** highlight the importance of layered, robust cybersecurity protection.

## What should the user do instead?

If you are ever instructed by a website to:

- Open an application on your desktop,
- Paste text into this application, or
- Execute any local command,

# Stop immediately.

Instead:

1. **Leave the website** straight away.
2. **Do not follow any further instructions.**
3. **Notify the vendor** using a known, legitimate contact method.
4. **Report the incident** to your internal it or security team.