Cybersecurity Digest

Bi-Weekly Update by O/o CISO of Meghalaya Rural Bank

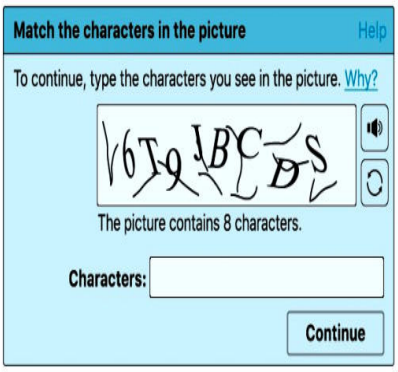
Volume 2 Issue 22

Date: 16-02-2026

CAPTCHA

A CAPTCHA test is designed to determine if an online user is really a human and not a bot. CAPTCHA is an acronym that stands for "**Completely Automated Public Turing test to tell Computers and Humans Apart.**" Users often encounter CAPTCHA and reCAPTCHA tests on the Internet. Such tests are one way of managing bot activity, although the approach has its drawbacks.

Although CAPTCHAs are designed to block automated bots, CAPTCHAs are themselves automated. They're programmed to pop up in certain places on a website, and they automatically pass or fail users.



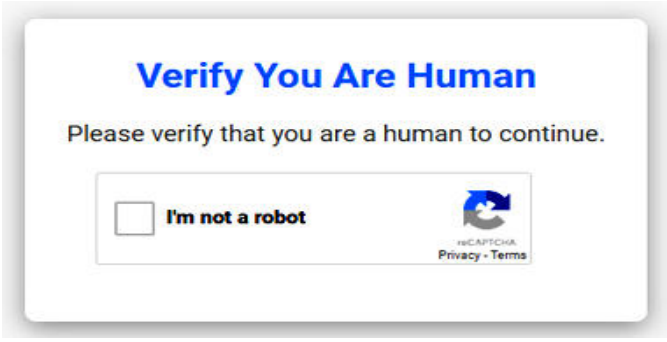
Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to identify letters. The letters are distorted so that bots are not likely to be able to identify them. To pass the test, users have to interpret the distorted text, type the correct letters into a form field, and submit the form. If the letters don't match, users are prompted to try again.

Such tests are common in login forms, account signup forms, online polls, and e-commerce checkout pages.

The idea is that a computer program such as a bot will be unable to interpret the distorted letters, while a human being, who is used to seeing and interpreting letters in all kinds of contexts – different fonts, different handwritings, etc. – will usually be able to identify them.

CAPTCHA ATTACK

Fake CAPTCHA attacks often begin with deceptive emails containing malicious links, misleading social media ads leading to fraudulent websites, compromised links on legitimate sites, or manipulated search engine results, and then the user is presented with a CAPTCHA, such as the one below.



Once users engage with the fake CAPTCHA, they may be prompted to copy and paste commands that seem harmless, but these can utilize PowerShell to run scripts in the background and execute malicious code, compromising their systems. Awareness of these tactics is vital for maintaining online security and avoiding these sophisticated attacks.

Socially engineered

The attack leverages our inherent trust in CAPTCHA challenges, exploiting the widespread assumption that CAPTCHAs are a security measure designed to protect us. This familiarity can lead people to let their guard down, blindly following instructions without critically evaluating the situation. Attackers also use tricks like adding harmless-looking text at the start of the command to hide the real code that does the damage

How to Spot Fake CAPTCHA

This is the classic CAPTCHA widget you've probably checked hundreds of times. But beware – a fake version may look identical. At first glance, the fake CAPTCHA may look identical to the real thing, and you'll be asked to check a box and confirm you're not a robot, just like you would with a legitimate CAPTCHA. But once you click through, instead of being presented with a challenge like identifying distorted text or selecting images, you'll be instructed to copy and paste a command into the Run dialog or a Command terminal; That's when you know you're dealing with a fake, as shown in fig.1.

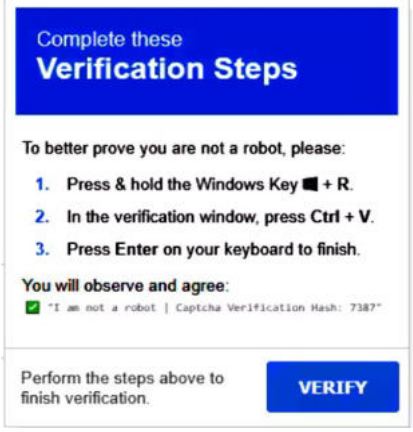


Fig. 1

Legitimate CAPTCHAs will never ask you to copy and paste commands, and if you do, you'll be executing a harmful command that could compromise your machine's security. The fake CAPTCHA wants to appear legitimate by showing you a preview of the command that you are being instructed to copy and paste, but this is a ruse. The real command being executed is obfuscated and is actually malicious, and may be hidden from view outside of the text field (as seen in fig.2, where the command appears to be a harmless verification ID).

As seen in fig.2, if the user pastes the command into the Run dialog and clicks OK, the malicious command is executed, potentially allowing attackers to access and control the user's system, install malware, or steal sensitive information, often without the user's knowledge or visible indication of compromise .

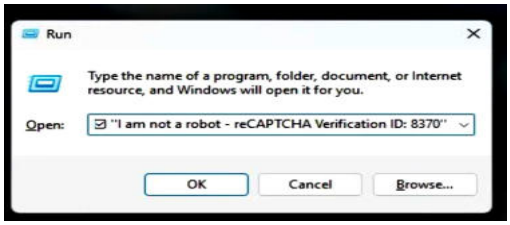


Fig. 2

Key Takeaways

Here are some ways to protect yourself:

- **Be aware of the Fake CAPTCHA technique:** Fake CAPTCHAs exploit trust of a familiar interface.
- **Never copy and paste commands from a website.** Legitimate verification processes will never ask you to run code on your computer.
- **Be wary of prompts to open Run or PowerShell:** These are not normal actions for everyday tasks, and could be a sign of a security threat.

What To Do If You're Affected

If you think you may have followed these steps and pasted a malicious command:

1. **Disconnect from the internet:** Immediately disconnect your device from the internet to prevent further communication with the attacker's server.
2. **Do not continue using the device** until it has been checked by your departmental IT staff.
3. **Notify your departmental IT staff or contact IT Helpdesk** to report the incident. Provide as much detail as you can about what happened.