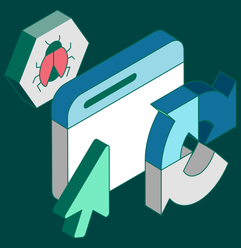


FAKE CAPTCHA SCAMS

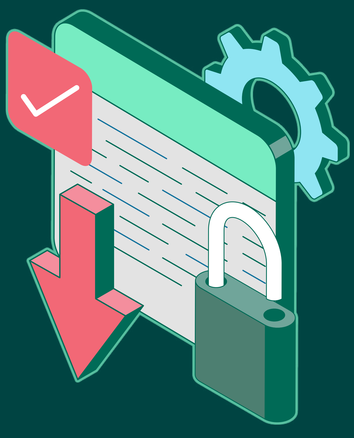
CAPTCHA stands for “completely automated public Turing test to tell computers and humans apart.” It is one of the most common security tools used online to distinguish real users from bots. CAPTACHAs typically involve simple tasks like checking a box, identifying matching images, or aligning a puzzle piece. Over time, many users have gotten so accustomed to these prompts that they complete them almost automatically. Malicious actors take advantage of this trust by creating fake CAPTCHA scams that trick users into performing tasks that put their devices and information at risk.

FAKE CAPTCHA, REAL THREAT

How it works: Cybercriminals use what looks like a CAPTCHA page or widget to get you to follow instructions or interact with pop-ups requesting access to sensitive features.

What it may looks like:

- A pop-up requesting notification permissions appears, accompanied by instructions guiding you to click ‘Allow’ to proceed.
- Another recent attack involves users being prompted to click a button that leads to malicious commands, or code being unknowingly copied to your clipboard.
  - On-screen instructions then guide them to use keyboard shortcuts, like opening the Run dialog, taking them out of the browser.
  - Following these steps, users unknowingly paste and execute the code, resulting in malware installation.



STAYING SAFE FROM FAKE CAPTCHA SCAMS

Be alert and implement the following best practices:

- Only solve CAPTCHAs on trusted, secure websites and never through pop-ups or redirects.
- A CAPTCHA will never take you out of your browser or require you to download something.
- Always pause and evaluate the situation before following instructions encountered online.
- Report any suspicious or overly complex CAPTCHAs to your IT team immediately.

Awareness of privacy and confidentiality concerns empowers you to harness the power of AI, safely!