

05.06.2025

Fake captchas

Seemingly harmless captchas can be used to also infiltrate your computer with malware. If you are surfing the Internet, suspicious prompts should make you wary.

Some websites use captchas, looking quite legitimate at first glance. They are meant for users to confirm they are no robots. In some cases, they are followed by another prompt – for instance to press a combination of the “Win-dows” and “R” key. Something which often goes unrecognised though: A command was already copied to the clipboard beforehand and can now be executed using this combination of keys. And this allows malware to infiltrate computers.

Such fake captchas usually appear on websites which have previously been hacked. Attackers change the site content and insert malicious scripts there – usually without the knowledge of the site operator.

If you are suddenly asked for further entries after following a captcha request, that should leave you suspicious and you should leave the site immediately.

What you can do:

- Do not press any key combinations or enter any further data when asked for by a website.
- Immediately close any windows with unusual captchas (for instance asking you to press a certain key combination).
- Use up-to-date antivirus software.