How fraudsters are bypassing CAPTCHAs to mess with your site

For attackers looking to access your website, a basic security test called CAPTCHA is a great line of defense. Since its creation in 2000, it has become increasingly sophisticated at catching advanced bots and keeping websites safe.

But we may be at the end of an era because according to Datadome, half of all CAPTCHA passed is completed by bots, not real users. That means the attackers controlling the bots can do everything from leaving spam comments and submitting invalid forms to abusing other services that your website provides.

In light of this, now’s a good time to understand how CAPTCHA works, how a CAPTCHA solver can bypass it so easily, and what it means for your website.

What exactly is CAPTCHA?

CAPTCHA is a descriptive acronym, and it stands for Completely Automated Public Turing test to tell Computers and Humans Apart. The CAPTCHA test allows human users to access a website but keeps bots out. CAPTCHA guards everything from spammy blog comments to even unauthorized downloads.

A CAPTCHA test will show the users images that are unreadable by bots. With letters, they are usually misshapen, washed out, or mixed up with a lot of gibberish, so only actual humans can interpret them. With images, there’s some sort of distortion that makes it harder for bots to use OCR.

Users need to input what they see into the provided field, and if they answer correctly, they are granted access to the protected web area. Simple bots will return irregular and incomprehensible letters or click the wrong images, making it obvious that they are not human.

Advanced bots, on the other hand, can use a variety of strategies to read these distorted images and bypass the test easily. As a result, more sophisticated CAPTCHAs, like Google’s reCAPTCHA, have been developed to increase website security.

Types of CAPTCHA

CAPTCHA is either text-based, picture-based, or sound-based, and the odds are that you've encountered all three.

Text CAPTCHAs

These are the most common, and they require you to look at the distorted text to identify the real message. Sometimes they are actual worlds, and other times, they are plain gibberish, distorted by shape, size, capitalization, or orientation.

If you fail enough text CAPTCHAs, you'll usually get a prompt to attempt a different method of verification, like a CAPTCHA image.

Picture CAPTCHAs

A CAPTCHA image can be quite troublesome when it doesn't look like there's a clear answer. A great example is a picture where you have to select all the grids with traffic lights, even though the light is split between two grids.

Luckily, you can always hit the refresh button to get another image with zero consequence. Or, you could try the audio CAPTCHA.

Audio CAPTCHA

With audio CAPTCHAs, users can listen to a short recording and type the word they hear. These are effective because bots can't use speech recognition to differentiate the pronounced characters from the background noise in the recording. It may be slightly uncomfortable to hear for humans, but audio CAPTCHAs are quite effective.

Google reCAPTCHA

Google reCAPTCHA is a more advanced version of the CAPTCHA tests. Instead of simply generating a verification test at random, it analyzes your mouse pattern and decides which test to show.

If the system thinks you're human, you'll get a simple "I"m, not a robot" checkmark CAPTCHA Otherwise, you'll have to complete a more difficult test like clicking all the boats in a group of pictures.

How do hackers bypass CAPTCHA?

Hackers now have an easier time bypassing normal CAPTCHA challenges, and here are some of the strategies they use.

AI

In his book, Deep Learning for Computer Vision with Python, Adrain Rosebrock lays out his strategy for bypassing CAPTCHA on the E-ZPass New York website. His approach included downloading hundreds of example images to train his system because he didn't have access to the source code, and then releasing the learned AI on the system.

CAPTCHAs with an open source code are, in theory, easier to crack because hackers can use the source to train their machine learning system to bypass CAPTCHA tests, regardless of the difficulty. Anybody can pass the exam if you know all the possible questions.

Click farms

Click farms are a little less sophisticated than AI, but they get the job done all the same. In a click farm, underpaid workers click away at websites trying to bypass security measures that are impossible for bots. So while a CAPTCHA may stump a bot, a human will solve CAPTCHAs without difficulty and in quick succession.

CAPTCHA hacking strategies

Hack Tricks lists some of the ways that hackers get around CAPTCHA easily. Some of them include checking your page's source code for CAPTCHA solutions (in case it's text) or using an old CAPTCHA value in case they get the same challenge twice.

Other CAPTCHA bypass strategies include

- Using OCR to read the characters on screen
- Checking how many images are being used and detecting them with MD5
- Sending the CAPTCHA parameter empty and seeing if that does the trick.

CAPTCHA solving service

Hackers may also use a CAPTCHA solver to gain access to your site. These CAPTCHA solution providers use a variety of approaches we've already listed, from AI to click farms and even simple API tools that can bypass CAPTCHA tests under specific circumstances.

These services can be called through simple browser extensions so that they get to work immediately the bot accesses your site.

Security Bugs

In 2018, a security researcher found a bug that allowed him to bypass Google's reCAPTCHA. The basic gist is that web apps using reCAPTCHA have to create the request in a specific way, and sometimes, the request is insecure. When this happened, attackers could bypass the reCAPTCHA every single time. (Andres Riancho)

The bug has since been patched, and it's no longer possible to recreate the reCAPTCHA bypass. However, this is a prime example of how attackers can exploit bugs and weaknesses to bypass your site's CAPTCHA.

Why Google reCAPTCHA is harder to bypass

What's interesting is that reCAPTCHA analyzes user macro behavior and adapts the challenges as necessary. So, for example, most bots will never get the "I'm not a robot" test because they don't engage with web pages the way a human does.

Even when they encounter the simple checkmark prompt, it's not as simple as ticking the box. If it were, the bots could grab the images on the screen, use OCR, and find out where to click.

These tests also analyze the pattern of mouse movement when you go to click. Human mouse movements are very clunky and jerky, and when the CAPTCHA detects that, it lets you through. A robot will move more smoothly and trigger a harder test.

What happens when hackers crack your CAPTCHA?

Any independent hacker can get past your CAPTCHA by simply filling it as a human would. The danger rises when they are able to bypass your CAPTCHA with bots. That means they can bombard your server with many requests, overload your resources, or possibly, steal your data.

Increased spam comments

Without an effective CAPTCHA "gatekeeper," you can expect spam comments that advertise everything from malicious services to other websites. If your website is set to approve comments first, they won't appear to the general public. However, you'll be drowned by dozens or even hundreds of irrelevant comments on the backend.

Invalid analytics data

Bots will skew the traffic on your web page and render your analytic data useless. If hackers figure out a way to get past your CAPTCHA, you may notice a spike in traffic with zero conversions or find that users are abandoning their carts, and you won't be able to figure out why.

Insecure shopping checkout

If you own an eCommerce website, a bypassed CAPTCHA means that hackers can now access user accounts, make purchases with stolen cards, and even access other sensitive areas of your website

Fewer web resources

With access to your website, bots will bombard your website, submitting connection requests and taking up finite resources. That means that legitimate users will have slowed or even nonexistent access to your website, which can be damaging for your business. Statistics show that 53% of people will go to a competitor if your website takes longer than 3 seconds to load (Digital).

What can you do about CAPTCHA bypassing bots?

Add reCAPTCHA to your website

reCAPTCHA is much harder to bypass than CAPTCHA, and iso it's a good idea to add it to your website. It’s free to use for the first 1 million assessments on your website per month, easy to install, and all you have to do is sign up for an API key pair for your site.

The specific instructions are laid out on the dedicated instructions page.

Bot Zapping by ClickCease

ClickCease’s Bot Zapping adds an additional layer of security to your website, stopping the most common forms of automated traffic from accessing your site. The service scans your visitor activity for telltale signs of bot presence and blocks them from interacting with your website.

That means even if they get through your CAPTCHA, Bot Zapping will identify and purge them from your website, allowing only genuine customers to get through.

The bottom line

Hacker tactics are becoming more sophisticated as they get better at bypassing simple defense systems like CAPTCHA, but luckily, you also have access to advanced measures.

Bot Zapping from ClickCease will make sure those automated programs don’t bypass captchas or mess with your marketing channels or forms.

Try ClickCease for free for 7 days and see how much of a difference blocking automated traffic makes to your site.