

CAPTCHA: Why Do We Need It?

Today, almost every website which has high internet traffic requires the user to enter the text displayed in a distorted image. This image is an example of CAPTCHA.

CAPTCHA stands for Completely Automated Turing Test To Tell Computers and Humans Apart. Recent tech-lingo also spells CATCHA as kaptcha.

A CATCHA is essentially a program which protects websites against bots by dynamically generating and grading tests. These tests are fairly simple for a human user, but nearly impossible for a bot to crack.

Applications of CAPTCHAs:

Preventing Comment Spam in Blogs

A popular trend in internet marketing is posting comments on blogs. Most marketers try to run a script on high-traffic blog sites, and get it to post an advertising comment. A CAPTCHA effectively prevents such scripts from spamming forums and blogs.

Protecting Website Registration

Any site which offers free registration to users runs the risk of losing thousands of accounts to bots. Sites like Yahoo, Gmail, MSN and many others, have now made it mandatory for a user to pass its CAPTCHA test to complete the registration process.

Protecting Email Addresses

Spammers run bots to crawl through websites and pick up email addresses. Websites today no longer display their email addresses openly; they secure it under a CAPCHA. Only if the user passes the test, the email address is made visible.

Safeguarding Online Polls

To ensure that online polls are an indication of users' opinions, and not a competition between rival bots, many poll websites take the help of CAPTCHAs. This guarantees that the votes are genuine and given by users with a valid viewpoint.

Preventing Dictionary Attacks

When bots try to hack into passwords, they launch a dictionary attack on the password field. Earlier, in order to prevent this, the site administrators would "lock" the account temporarily, after a certain number of wrong attempts. But this gave malicious bots the freedom to intentionally cause certain account to get "frozen" or "locked".

CAPTCHAs are now popular in such scenarios. Instead of locking the account, the administrator now poses a CATCHA to be solved, after the quota of unsuccessful logins has been run. This effectively outsmarts the hacking bots.

The Cat And Mouse Game

The tug-of-war of Artificial Intelligence between CAPTCHA generators and hacking bots is continuous phenomenon. When the first CAPTCHA was released in 2000, it was a major technological breakthrough. And very soon, the first hack was made too, and scored over this CAPTCHA. The CAPTCHA then re-invented itself to cover its earlier flaws. And bot writers began to strive to crack it...

Till date, this intriguing cat-and-mouse game continues...

About the Author

A software programmer who pursues her dual passions of programming and writing.

Source: <http://www.topsub.com>