Sur.ly Blog

I am not a robot: How to stop human-generated fake user registrations on any platform

BY SUR.LY TEAM ON AUGUST 22, 2017 | NEWS AND ANALYTICS

If you run a free membership site of any kind, then you surely have a first-hand experience of dealing with spam signups. Such fake registrations are a pure garbage that adds no value to your user base, ruins the overall picture of your audience, and can do no good to any marketing efforts: the more fake/dead accounts your database contains, the harder it becomes to study registrant demographics, build customer relations, and target your propositions at specific user groups.

The issue is as old as the Web itself, but there is no complete solution on the way: once the industry comes up with another 'bulletproof' spam protection tool, it's just a matter of time for spammers to invent a tricky way to override it, so this race will probably never end.

The best thing site owners can do about the issue is to build the right mix of preventative measures to find a balance between blocking fake users effectively and 'scaring' legit users away. For example, CAPTCHA services went through a few turns of evolution before Google has recently created the Invisible reCAPTCHA which is 'tough on bots, easy on humans' meaning it can stop spambots, but stays invisible for regular users (so it cannot resist human spammers too – sorry, Google).

There are tons of conventional tips and tools to cope with bot signups, but let's take a closer look at the problem – which of those popular methods are effective enough to **stop human spammers**?

Analysis: regular anti-spam tools vs. human spammers

1. **Spam proof user registration forms**: they always feature some CAPTCHA-type human verification testing (solving quizzes, math problems, etc). It may include 'honeypot' technique that uses invisible fields to distinguish bots from humans (spambots will automatically fill those fields in, and thus disclose themselves) – it doesn't bother users like a CAPTCHA, so might lead to a better form conversion rate. Although such forms can perfectly rebuff armies of generic spam bots, they obviously don't stand a human spammer.

CAPTCHAs may go tough on legit human users too

2. **Email or phone verification**: when you ask a user to complete their registration by clicking a confirmation link in the email, spam-bots are less likely to get through this security barrier, but it won't stop a human. A more advanced method, like sending SMS or voice-based passcodes, can be much more effective: it can prevent not only automated spam attacks but human-generated too, as not many spammers are ready to disclose their phone numbers (there are still many countries where you need an ID card to start a mobile subscription). While it can work well for large projects, this method may appear too expensive for smaller sites and communities.
3. **IP blocking**: there is a number of smart CMS plugins that check user IP addresses, and ban any activity from the blacklisted ones. Web admins can even block entire countries (or other locations) if they are not interested in foreign users, so theoretically no local spammers can hit the site. In reality, professional spammers or advanced bots can overcome these IP restrictions with ease: they may be supported by proxy-list trawlers which can identify dozens of IP proxies and switch between them to get masked in a matter of seconds.
4. **Manually moderating user submissions**: it will require a moderator to approve each registration request before the new user can join the website (or publish content there). It makes sense for websites with a relatively small number of daily registrations, but it can be a time-consuming and irrational practice when it comes to dealing with hundreds of new users per day awaiting verification. Anyway, it never guarantees that human spammers won't be overlooked, as their profiles may look quite legitimate (properly or creatively filled, such accounts may not look like a spam-type profile generated by a bot).

As you can see most of the traditional anti-spam tools are built to fight bots, not human spammers that are much trickier than any automatic spam script could be.

Well, in order to defeat spammers, we need to get to the root of the issue first...

How to make a site immune to human-generated spam?

But why spammers are so persistent in their efforts to infuse your site with their fake data? There are two main reasons for it:

- Scamming/spamming your legit users.
- Spreading or publishing outbound links to their lame/toxic sites (so called link spam).

Posting links allows them to pass a portion of ranking power from a public website with a greater ranking potential to a smaller site(s), so the last one can rank better and increase its position in SERP. The bigger site, being a link juice donor, gets nothing in return, except for junk links. So unjust!

Sometimes, it's not even necessary for a spammer to post links: on some websites, the user registration process ends up with a creation of a personal page/album including a few essential fields – some of these fields may be of hyperlink type (for example *user's homepage*). Spammers could quickly fill it in, say 'done!', and then go no further from this point, as they've already created a channel for link juice to flow! (the only effective way to stop such parasites is to auto-remove their profiles after a period of inactivity).

Well, there is something else you can do about the issue: give all your unnatural or toxic links to Sur.ly! It will make your site totally immune to link spam breaches so no human spammers can benefit from posting their links. Actually, with Sur.ly there will be no more toxic/bad links on your site (at least for Google robots or your real users that will get an extra protection set for their computers).

Back to Blog Tweet Like
0 Comments blog.sur.ly Disqus' Privacy Policy Vlad Vortex
Recommend Tweet Share Sort by Best
Start the discussion…
Be the first to comment.
Subscribe Add Disqus to your siteAdd DisqusAdd Do Not Sell My Data

Recent posts

How To Identify And Neutralize Phishing Attacks

POSTED ON SEPTEMBER 22, 2017

Everyone who often deals with the Web has ever heard the term 'phishing attack'. Today we will explain what a phishing attack is, reveal its mechanisms, and give you effective tips on how to recognize and rebuff any phishing attempts.

How To Keep Visitors On Your Website Longer?

POSTED ON SEPTEMBER 14, 2017

It comes as no surprise that every website owner who worked day and night to build his/her project is always in search of 'holy grail' trying to invent a better way to retain visitors, get people interested, focused on the site's content, and then straightforwardly converted into sales or sale leads.

Sur.ly Surfguard is here!

POSTED ON SEPTEMBER 1, 2017

Sur.ly Surfguard is here! It's a browser addition powered by our web safety platform, which lets you preview status of a link before clicking on it. If a link is unsafe, you'll get a pop-up notification when hovering your mouse over it.

Newsletter

Subscribe to our newsletter to follow our updates, announcements and promotions.

E-mail Subscribe

Sur.ly News

- Sur.ly Surfguard is here! It's a browser addition powered by our web safety platform, which lets you preview status of a link before clicking on it. If a link is unsafe, you'll get a pop-up notification when hovering your mouse over it. — 01 September 2017
- Meet the Sur.ly blog! A place where we'd be happy to share our expertise, useful tips, analytics, and best insights into the world of SEO, link building and spam-fighting. — 16 August 2017
- Updated FAQ sections up-to-date answers and instructions are ready to guide you on Sur.ly's features and best practices. — 05 May 2017

© Sur.ly, 2012—2020