Hackers Shut Down ProPublica's Email For a Day. Here's How to Stop Attacks Like That.

by **Julia Angwin**, Nov. 13, 8 a.m. EST

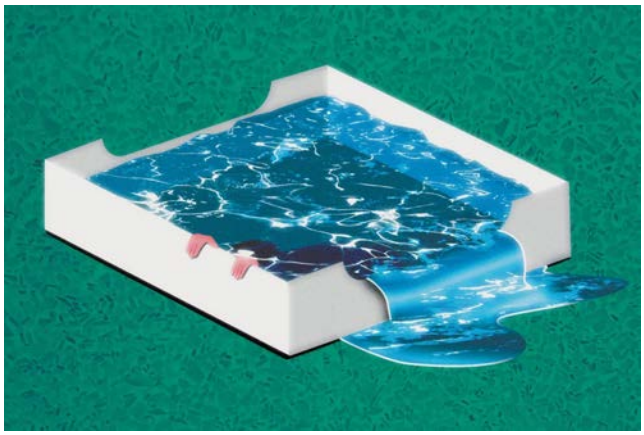
This post originally appeared in our weekly newsletter. Sign up here.

In August, my email was attacked. Hate groups overwhelmed my inbox and the inboxes of two of my colleagues, and shut down ProPublica's email much of the day. (I wrote about this incident in a previous newsletter.)

This week I wrote about the low cost and high effectiveness of such attacks. The assault on ProPublica — a type known as "email bombing" or "subscription bombing" — exploited the proliferation of websites that offer email sign-ups. The attacker uses an automated program — which costs just $5 on online hacking forums — that enters the victim's email into every single sign-up form it can find. Then the victim's inbox is deluged with emails seeking to confirm the sign-up.

In other words, my story shows how harassers have found ways to exploit yet another opening in web infrastructure. And despite its limited sophistication, email bombing is extremely difficult to defend against.

A widely respected anti-spam service recommended that the "single best thing that can be done" would be for email lists to include a test known as a CAPTCHA to distinguish between human and automated sign-ups. Most internet users know CAPTCHAs as the squiggly words or sequence of photos they are asked to identify.



Cheap Tricks: The Low Cost of Internet

Unfortunately, not every web form uses

for people to receive their missives, especially when the people harmed by the sham sign-ups are not their clients.

The email industry is working on a solution that it hopes will limit these attacks. The Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) has asked bulk email senders to identify subscription confirmation emails with a special technical header. That would allow email services to filter and block confirmation emails during a subscription attack.

with email bombs and Twitter bots and covered their tracks.

Despite Disavowals, Leading Tech Companies Help Extremist Sites Monetize Hate
Most tech companies have policies against working with hate websites. Yet a ProPublica survey found that PayPal, Stripe, Newsmax and others help keep more than half of the most-visited extremist sites in business.

But not all email senders are likely to adopt the standard, and not all open web forms are managed by bulk email senders. So here are a few things I learned in my reporting that could help guard against "email bombs."

Easy — But Annoying — Tip

Do you run a website or a newsletter or some sort of listserv? Is CAPTCHA turned on? Turn it on. We know it's not the easiest or prettiest thing, but if you're interested in guarding against this attack, that's a measure you can take.

Do you sign up for newsletters or listservs? Do the newsletters or listservs you sign up for have CAPTCHAs? If not, that could be a problem. Reach out to them and encourage them to implement CAPTCHAs, or the technical header, or both. Forward them this newsletter or send them my article.

Pro Tip for (WordPress) Websites

Many of the confirmation emails that we received were from websites running WordPress software. WordPress allows users to register for an account, for purposes including posting comments on a blog.

If you have a WordPress site, you can turn off user registrations — if unneeded. You can also install a CAPTCHA on your sign-up form. These actions would help stop perpetrators from deploying an "email bomb" using your website.

Unfortunately, none of these solutions is very satisfying. At least people are starting to

of a launching pad for hate and harassment of all kinds.

We also shared tips with you last week regarding your personal internet security. Check those out here.

Julia Angwin

Julia Angwin is a senior reporter at ProPublica. From 2000 to 2013, she was a reporter at The Wall Street Journal, where she led a privacy investigative team that was a finalist for a Pulitzer Prize in Explanatory Reporting in 2011 and won a Gerald Loeb Award in 2010.

@JuliaAngwin