Carding & CAPTCHA: Protecting Your Organization from A Fraudulent Payment Attack

Your payment processor is vital to the smooth functioning of your organization, whether you use PayPal, Stripe, WePay, Square, or another service. What might happen if your payment processor went down for a day or two? There is a common type of fraudulent credit card attack, known as carding, that can disable your ability to accept payments within hours, as one of our grantees recently discovered. In a carding attack, a malicious actor uses bots to generate and test credit card numbers by charging small amounts and seeing which cards work; donation pages are the perfect target for these rapid-fire fake transactions. You can take simple anti-spam steps to protect your donation portal and protect yourself from a carding attack like this one.

Anatomy of a Carding Attack: When 1,000 New Donors is a Problem

It started with some $1 donations, on a Saturday morning when no one would be monitoring work email. At first thought, the organization’s director believed the donations came from a grassroots campaign sparked by a recent news article about the organization. When the $1 donations started reaching into the dozens, and then hundreds, however, she became suspicious. The payment processor began to flag the transactions as suspicious as well. Within two days, the account was suspended – on the eve of a fundraising event, when the organization relies on their online payment portal to accept donations in real time.

What were these $1 donations? All of the transactions used the same mailing address, and same phone number, but different names, email addresses, and credit card numbers. The email addresses looked off – the first donation had an “@armyspy” domain. Whenever you see something suspicious, trust your gut – a DuckDuckGo or Google search can reveal a lot about whether the email is legitimate or not. A search quickly revealed that the “@armyspy” domain is part of a fake email generator network. Later email addresses were all random numbers.

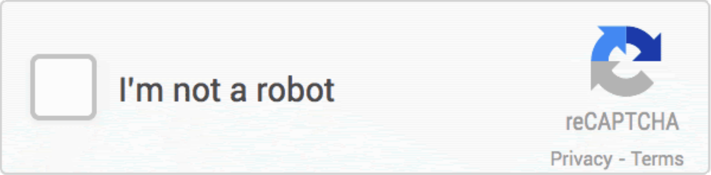
The transactions were relentless as the attacker generated hundreds of credit card numbers to test. If the credit cards worked for a $1 transaction on the nonprofit’s website, the attacker knew that card would work to make high-dollar purchases on other sites, too.

By the time the payment processor suspended the account, the attacker had attempted 1,727 fraudulent transactions, all $1 donations. About 200 of those transactions had successfully processed. The payment processor laid out a few steps for getting the account reactivated; the most important was installing a fraud prevention tool like a CAPTCHA and refunding all 200 of the successful charges.

In an attack like this, the organization is almost always collateral damage, a tool for the attacker to use to identify the real target: credit cards that work. Nonprofit donation pages are a convenient tool for this kind of fraud, since the person running the transaction can choose the amount to be charged. Did the malicious actor choose to turn his credit card bot loose on this organization's donation page because they were opposed to the organization's mission? It's impossible to know for sure. One clue is that the donations all came through a donation page created for a special event, a Reddit AMA that the organization hosted about a year prior. The attacker must have found the organization through that link. There's no way to know if they were already looking for a carding target, or if they found the link and then decided to do a carding attack.

Attack Resolution

The good news is that it's very easy to install anti-spam tools on your donation page. These anti-spam tools can be installed by the person who built your website or donation form, or you may be able to do it yourself if you use a user-friendly form plugin. There are two main kinds of anti-spam tools, which we'll explain below: CAPTCHAs and honeypots.



You've probably seen a CAPTCHA before – it's a tool made by Google that asks you to complete an action to prove you aren't a bot. If the activity from your computer seems human, you'll usually just have to check a box. If you are using a software or computer that makes you look suspicious according to Google's algorithm, you'll have to complete a puzzle. Instructions for adding a CAPTCHA to WP Forms for WordPress users can be found here, for example, and for Form Blocks on SquareSpace here.

CAPTCHAs are, overall, very effective, and Google is constantly improving their technology to thwart bots. However, CAPTCHAs can affect the accessibility of your site, since some people with disabilities are unable to complete certain CAPTCHA tasks. In response to the accessibility issues, the newest version, reCAPTCHA v3 or "Invisible ReCATPCHA", does not require users to complete any tasks unless Google's algorithms identify them as suspicious. If the user is flagged, they will have to complete a traditional CAPTCHA puzzle.

Other companies are creating alternatives to Google's CAPTCHAs, and one of the most prominent is hCaptcha.

An alternative to CAPTCHA is an anti-spam honeypot. When a bot completes a form, it scans the HTML of the webpage to automatically find and fill all the fields. An anti-spam honeypot is an extra field that is coded into the page, but hidden from view. The field is also hidden from the tab command and from auto-complete. Only spambots can read and complete the field. A honeypot field may be an obviously fake checkbox saying "Contact me by fax only", as in this example. Any bot that checks the checkbox will automatically be blocked. Honeypots can be set up to accommodate screen readers, used by visually impaired people, as well. This is now a default option on some webforms, like WPForms for WordPress users, and can easily be enabled in other form plug-ins.

As soon as the organization suffering the carding attack set up a CAPTCHA, the attack stopped. The next step was reactivating their account. After a couple of phone calls and emails with the payment processor, the account was restored after being down for about 36 hours. This wasn't the end yet, though: the director had to quickly refund all 200 fraudulent charges, one by one, to avoid any chargebacks from the real card owners, who would likely dispute the charge once they discovered it. Chargebacks at this payment processor cost $20 – so the organization stood to lose a significant amount of money.

What can you do to prevent this kind of attack?

Here are a few things that your organization can do to prevent carding attacks:

- Make sure you have a CAPTCHA like Google's or hCaptcha's, anti-spam honeypot, or both installed on every form on your website – especially donation forms.
- Talk to your payment processing company about any anti-fraud services they offer on their end. Write up a plan of action if your website is the victim of a fraudulent attack.
- To protect against this and other kinds of denial of service attacks, you can also install DDoS protection, which defends your site against malicious bot abuse. Nonprofits have a few options to choose from, including the non-profit version of CloudFlare, Google's Project Shield, the free non-profit tier of Deflect, or paid secure hosting from Quirium.

If you are the victim of a carding attack, be communicative with your payment processing company. Get clear instructions on what you need to do to reactivate your account, and don't be afraid to ask all your questions. Ask if you have to refund the transactions yourself, if there is a bulk way to do that, and check about any anti-fraud services that they may offer to further protect your account in the future.

If you are an abortion access organization that needs help with any of these steps, send us an email!