Protect Your Web Form From Bot Attacks

This article applies to:

List bombing occurs when an email address was submitted to your web form by someone other than the owner of the address and you unknowingly sent unsolicited email. While one or two instances will surely go unnoticed, this problem can become especially significant if it occurs in bulk.

The Cause: Subscription Bombing

The most prevalent cause for this is what's known as "subscription bombing", which is an attack designed to overload a recipient's inbox with unsolicited email, thus rendering their inbox useless (imagine how useful your inbox would be if it received over 100 emails per minute). The attacker essentially weaponizes your marketing automation by using a script or bot to submit the email address of the target, or more often multiple targets, into as many web forms as possible. The attacker then relies on your email automations or broadcasts to contribute to a barrage of unwanted emails aimed at their target - all without your knowledge.

The Impact: Greatly reduced email deliverability

Allowing your forms to be used as an attack vector to send unsolicited email, especially in significant volumes, negatively impacts your (and our) email sender reputation with mailbox providers (e.g. Gmail, Yahoo, etc.) and blacklisting providers (e.g. Spamhaus). Because sender reputation is so critical to inbox placement, you are effectively held accountable for the all email that you send - including email sent because of a bot attack on your web form.

The Solution: CAPTCHA and COI

- Use CAPTCHA- Google's ReCAPTCHA is enabled by default on web forms created with Infusionsoft, but you will need to setup CAPTCHA on your own if you use 3rd party web forms.
- Use Confirmed Opt-In (COI) AKA "Double Opt-In" (DOI) - When used correctly, a COI sequence will send no more than one email per form submission per recipient. While this doesn't completely stop you from unknowingly sending unsolicited email, it does help limit the amount of unsolicited email that you send, thus reducing the potential damage to your sender reputation. In this way, COI can help to prevent a subscription bombing attack from compounding.

Email industry experts and blacklist moderators agree: the best defense against subscription bombing is using both CAPTCHA and COI. Remember, while Infusionsoft does not require the use of CAPTCHA or COI, we do require that you obtain explicit permission to send email, and unsecured web forms provide the possibility for you to unknowingly violate that requirement.