POSTUP SOLUTIONS

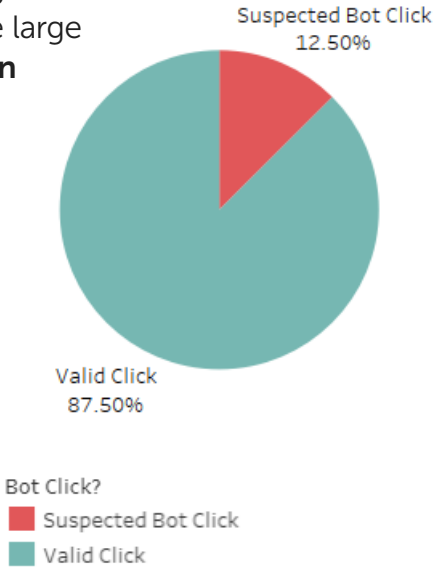
SECURITY APPLIANCE DETECTION

PostUp

Curb inflated click rates with PostUp's security appliance detection.

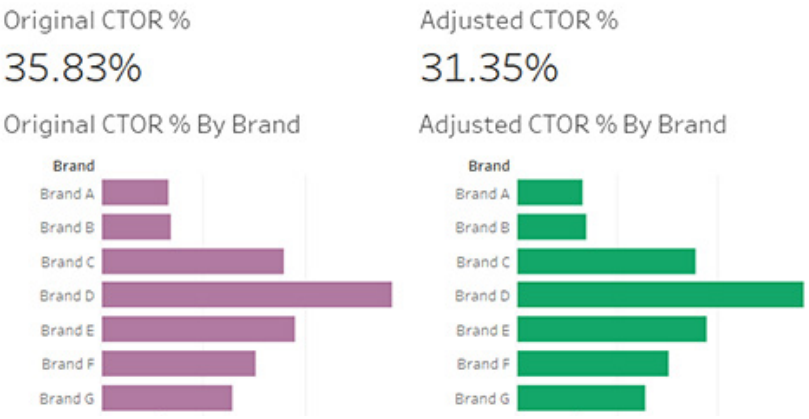
If you're reading this from work, odds are your email inbox is protected by security software.

These sophisticated security appliances assess potential threats by "clicking" email links to determine if they link to malware or phishing sites. To prevent fraudulent senders from detecting (and circumventing) security, appliances try to emulate human behavior. Unfortunately, for legitimate senders like you, it also inflates click-through rates—especially if you have large corporate, educational, or nonprofit audiences. **In the arms race between scammers and security, your reporting is collateral damage.**



That's why PostUp has developed a way to reliably detect and address security appliances. PostUp uses invisible "honeypot" links to identify, flag, and track email domains protected by security appliances. That way, you can:

- Know your percentage of appliance-protected recipients
- Isolate protected domains from your click reporting
- Estimate true click-through rates for your protected recipients



We've found that up to 10% of email addresses on our clients' lists are behind security appliances; **in one case, this 10% accounted for 77% of a campaign's total clicks.**

With appliance detection, you get the most accurate click-through reporting, even as the war for the inbox wages on.

Contact us to learn more: 877-250-2922 | info@postup.com | postup.com