Account Takeover Protection

Phishing sites are the launching pad for account takeover campaigns

Account takeovers are an ever-present challenge for online businesses and continue to be a thorn in the side of security teams to detect and stop them. Phishing sites posing as your brand and aiming to steal account credentials remains the primary attack vector for fraudsters to gain access to customer accounts inside your online business. And fraudsters are smart. Once credentials are stolen, users are often redirected from the phishing site to the real site leaving users oblivious while fraudsters cover their tracks. These sneaky techniques are rampant, and virtually impossible to detect and prevent without proper mechanisms in place.

Use Bolster for early detection of compromised accounts

With our Account Takeover Protection (ATO) solution, you'll get immediate and pre-emptive capabilities. The solution is powered by a real-time detection engine that scans the Internet for credential theft phishing sites rendering verdicts in milliseconds. Detection of phishing sites trigger automatic submissions to global blocklists and zero-touch takedown mechanisms to stop attacks in their tracks.

Our ATO solution will also actively monitor your inbound website traffic, looking specifically at the URL referrer entries in your web logs. The system will scan these URLs in real-time to assess if users are coming from active phishing sites and are potentially compromised. When compromised conditions are detected, the system will initiate a lock on the account or issue a password reset while also executing a takedown of the phishing site.

Identify Compromised Users

Use HTTP referrer logs to identify potentially compromised users & trigger password resets or account locks.

Detect & Block Phishing Sites

Use with phishing pixel beacon to identify, block & take down phishing sites & lock affected accounts.

Execute Zero-Touch Takedowns

Automatically take down phishing sites as they are detected, preventing one account takeover from turning into thousands.

Easily Integrate with Operations

Augment security operations with real-time detection & automated protection in just a few steps.

BOLSTER

NEXT GENERATION
Fraud Prevention Platform

Detect & stop account takeovers from taking over your business.

Ultra-fast, Ultra-accurate Detection	**<100ms** Fraud detection verdict	**1/100,000** False-positive rate	**60 sec** Mean Time to Response (MTTR)
Fully-automated Zero-touch Takedowns	**2 mins** Avg API based takedown time	**95%** Without manual intervention	**6.5 sec** Submission to global blocklists

How it Works:

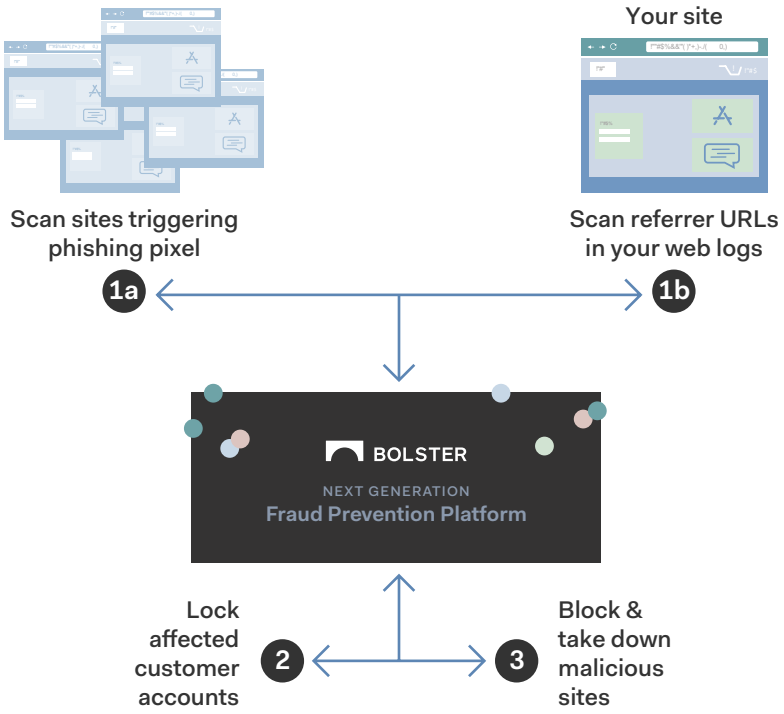
1a. Use with phishing pixel beacon to detect phishing sites in real-time

1b. Scan referrer URLs in web logs to detect traffic incoming from phishing sites

2. Use account level detection inputs to automatically initiate password resets or lock the affected customer accounts

3. Use site level detection inputs to automatically take down active phishing sites

Stop account takeovers with AI-driven detection & fully-automated protection



Protecting Leading Brands Around the World

Booking.com Dropbox change.org fitbit

LinkedIn twilio Uber zoom

About

Bolster builds AI/ML technology to protect regular citizens from bad actors on the internet. Your favorite brands from technology to eCommerce trust our software to detect and takedown threats that might attack their customers, employees, or partners.
Learn more at: www.bolster.ai

4966 El Camino Real, Suite #101
Los Altos, CA, USA 94022
info@bolster.ai