

Email 1

Subject: Does [Company Name] Have All the Top 5 Security Technologies?

Hi [First Name],

According to industry studies, bot mitigation is one of the top five cyber security recommendations to protect financial organizations.

Web application firewalls (WAFs) are critical network components, but they don't withstand sophisticated bots. Today's bots routinely bypass WAF by acting like legitimate users and abuse website logic and APIs to infiltrate your website and commit fraud.

Without insight into who or *what* is accessing your website customer login pages and online information, good bot, bad bot, and human traffic all look the same.

Identify Bots Accessing Your Data Right Now

Read our blog [Good Humans vs. Bad Bots](#) to decipher between legitimate users and potential attackers and see how to keep your data protected.

- BotRx

Social Post:

The @USTreasury views cyberattacks as one of the key threats to U.S. financial stability. With #bots becoming more sophisticated, it will require bot mitigation solution to protect websites, #applications, #IoT devices, and our country. Learn how to spot #bot traffic in your network.

Email 2

Subject: [Company Name] is 300x More Likely to Be Attacked, Find Out Why.

Subject 2: Do You Have Bad Bots?

Hi [First Name],

Bad bots love doing financial services online, just like your real customers. Nowhere is automated fraud and credential stuffing more prevalent. But you can stop them.

Your customer assets and account data is valuable to hackers—that's why bots are more attracted to financial organizations like yours. Recent studies prove it: **financial services firms fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries.**

"BotRx's solution is very advanced and protects applications and websites at the same time, securing user profiles, users' stored value, individual funds, and cash flow. " - Kenny Chen, FETC CIO

Bad Bot Threats Are Growing

Read our benchmark data report to learn what we're seeing in organizations like yours.

- BotRx

[Try BotRx's Free, Lifetime Access](#) to Detect and ID the Bots Attacking Your Website.

Social Post:

Financial services firms are 300 times more likely to experience a #cybersecurity attack because of the value of their #data. That doesn't mean attacks have to be successful. Read our benchmark data report to see what you're defending against.

Email 3

Date: 9/26/2019

Subject: Detecting Bot Attacks is Easy and Free (and Critical for Financial Organizations)

Subject 2: This is Your Chance to Stop Bad Bots

Hi [First Name],

When it comes to bot attacks, financial services is in the top 5 targeted industries.

Why? People are doing a majority of their banking and completing financial transactions online. Your customer accounts and their personal data is worth A LOT of money to fraudsters on the darknet.

The best news? Bad bots are both easy and affordable to stop when you have the right bot detection and mitigation solution.

Detect Bots Today

Why not [find out RIGHT NOW](#) what bots are attacking your website and putting your customers at risk? It's free, no strings attached.

- BotRx

Social Post:

Stealing personal data means a big payday for fraudsters and #financial is one of the top 5 industries targeted by bad #bots. Find out if your organization is under attack RIGHT NOW with free, lifetime access to BotRx DeTx.