keepnet

Bot Activity Explained

What is Bot Activity?

Bot Activity refers to the non-human activity on a simulated phishing email. For example, when your security solutions check links within an email to protect your organisation from potential threats.

By default, Keepnet hides bot activity from your phishing campaign reports so you can focus on when your employees are clicking on links

Security Tools

Security tools check emails as they come into your inbox and also when your employees engage with the Phishing URL within the email

Browser

Some browser extensions will run checks on URLs you are engaging with. This can be for security purposes or marketing purposes.

Type of security tools

Email security scanner, Proxy, DLP systems, Content filters and some new API tools

And more!

How Keepnet identifies Bot Activity

A1

Unusual User-Agent Interacted: Triggered when an atypical or suspicious user-agent (browser identifier) is detected.

A2

Honeypot Link Reused: The hidden phishing link inside of the email clicked multiple times by the same IP and user-agent within 5 minutes—indicating automation

A3

Same-Second Activity Spike: Multiple activities occurred at the exact same time, which is unlikely for human users

A4

Stop Bot Activity Challenge Failed:

A4.1 – The phishing link was clicked, but the invisible browser javascript challenge was not passed.

A4.2 – The browser failed to load required scripts that a real user's browser would normally execute**.**

A1. Unusual User-Agent Interacted

Explanation

Whenever a link is clicked by a browser, the browser calls our servver and shares the browser information. Bots have a different user agent to employees. Any unusual user-agent is marked as bot activity

Example

An employee sees a suspicious link in their inbox. Instead of clicking the link, they share it to Slack.

Slack may then check the link. When the browser calls our server, the user agent will say “Slackbot” (or something to that effect1)

These unusual user agents are marked as bot activity

A2. Honeypot Link Reused

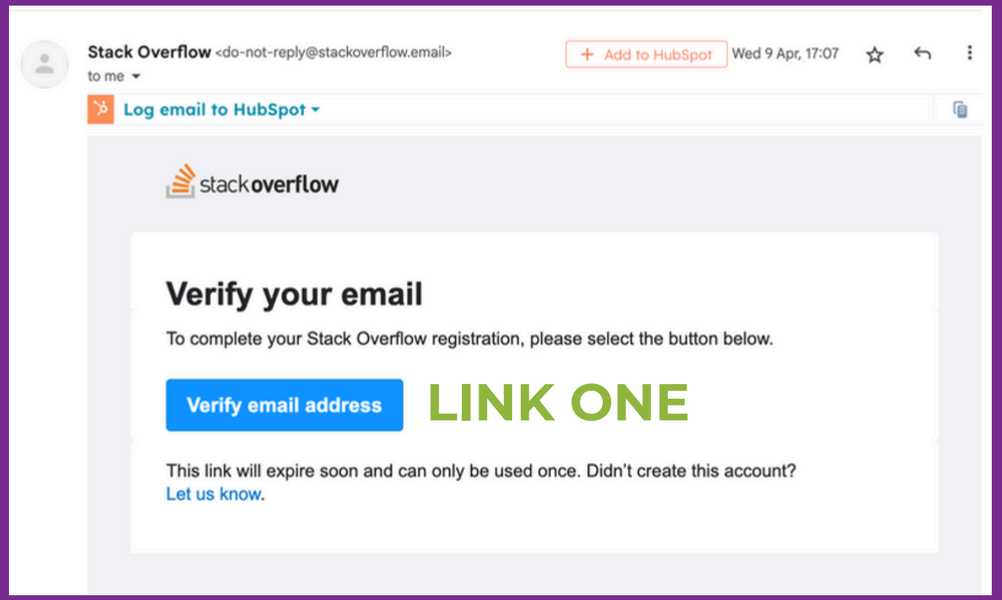
Explanation

Within a Keepnet simulated phishing email are **TWO** links

LINK ONE: The Phishing URL employees see in the body of the email

LINK TWO: The Honeypot link in the email header information. Employees do not see this in the body of the email

Keepnet knows a security tool is checking the links within an email when the honeypot link is being clicked. This is a clear indicator that an employee is not interacting with the email



A3. Same-Second Activity Spike

Explanation

Some security solutions will cause several clicks within the same second, Something almost impossible to recreate manually by human activity.

In this instance we can confidently say that the link is bot activity.

Example

When a security solution checks the email, they will check both the phishing URL link and the honeypot link simultaneously, within the same second

Without this rule, we would show one bot activity (honeypot link clicked) and one human activity (phishing URL link clicked).

Introducing this rule allows Keepnet to confidently determine when a security is checking all links in an email and mark all instances of click in the same second as bot activity.

A4. Stop Bot Activity Challenge Failed

Explanation

Captcha = Invisible puzzle

Keepnet use CloudFlare’s captcha service on all landing pages by default.

CAPTCHA is typically not passed unless there's active browser interaction. Previews or background link checks (by mobile, mail clients, or scanning apps) won't complete it. These previews can trigger a page load, but not CAPTCHA resolution, which leads to a failed challenge

Rule A4.1 = Failed to pass captcha
Rule A4.2 = Failed to load captcha

A4.1 Stop Bot Activity Challenge Failed

✅ Rule A4.1 – CAPTCHA Loaded but Not Solved

Triggered when the phishing simulation landing page is accessed and the CAPTCHA is successfully loaded, but never solved. This typically occurs when:

- The URL is previewed by mobile email clients, messaging apps, or QR code readers, which partially load the page but do not allow full user interaction.

Use case: This helps identify passive engagement with the phishing simulation - often by tools that opened the link without taking further action - distinguishing them from human activity.

A4.2 Stop Bot Activity Challenge Failed

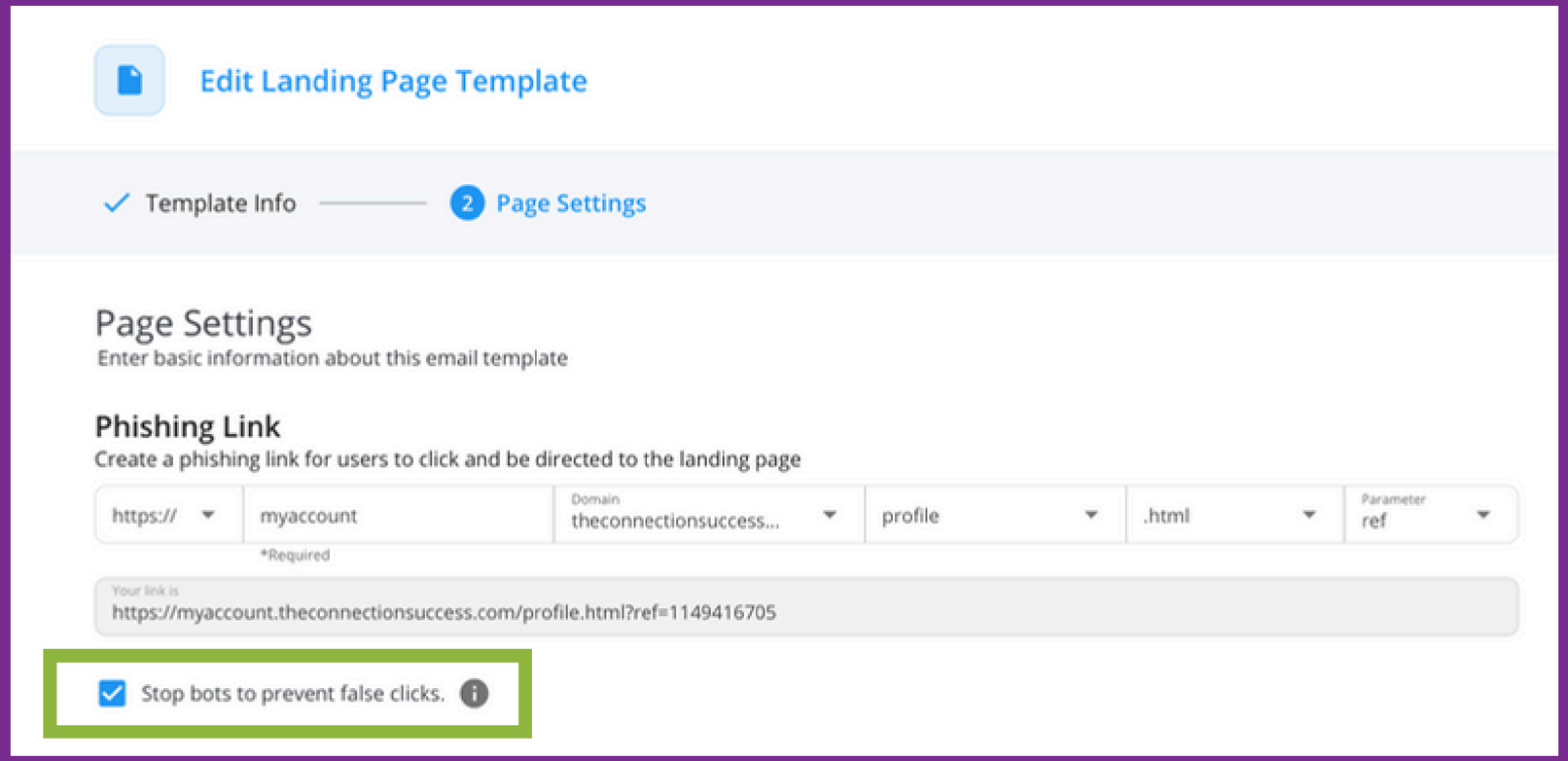
✅ Rule A4.2 – CAPTCHA Not Loaded

Triggered when the phishing simulation landing page is accessed, but the CAPTCHA challenge is never initiated or loaded. This typically occurs when:

- Security scanners (e.g. Fortinet, VirusTotal, etc.) or email security gateways access the URL using non-browser-based methods
- Bots or automated systems fetch the page content without rendering scripts or front-end elements required for CAPTCHA to load.

Use case: This indicates that the URL was scanned or tested by a system without full browser capabilities—often a security product or automated threat detection engine.

A4 Stop Bot Activity Challenge Failed



You can turn the "**Stop Bot Activity**" off for landing pages if you would like to stop this rule from running.