27
Jan

Phishing (/category/phishing)

How to Avoid Phishing Simulations False Positives?

In a survey (https://www.forbes.com/sites/edwardsegal/2021/11/11/how-cyber-thieves-are-ramping-up-their-phishing-attacks-against-companies-and-organizations/?sh=4d61fe8f20a6) taken last year, 35% of organizations reported being targeted by at least one phishing attack. While phishing remains a pervasive threat, many organizations have started implementing phishing simulations to measure employee security awareness. Still, those organizations have also struggled to deal with phishing false positive clicks leaking into their data.

Security tools in the environment can automatically scan links and make it look like a user failed to spot a phishing email when, in reality, it was a bot-click, causing the user to fail a test unfairly.

This article will define and examine bot-clicks and showcase how your organization can avoid phishing false positives in phishing simulations.

What is a Phishing Simulation?

A phishing simulation (https://terranovasecurity.com/phishing-simulation/) is a test where an organization will send employees simulated phishing emails that impersonate real-world scams to see how many employees click on a malicious link. Users that click are deemed to have failed the test, as they've been tricked by common cyber threat tactics. Had it been an actual phishing attack, sensitive information may have been compromised.

What is a Bot Click?

By measuring user clicks, an organization can deem how effective employees are at spotting scams, whether they're following the latest security best practices, and if they need access to additional security training opportunities.

However, third-party software solutions and security tools have bots that can click on all the URLs in an email in a sandbox environment. This process is put in place to make sure there's no malicious content within the email.

This practice, while common, can artificially inflate the results of a particular phishing simulation and thus skew the resulting data.

What is a Phishing False Positive?

Bot clicks that occur in a safe environment to ensure that this is not an actual phishing attack can be categorized as phishing simulation message clicks, even if they don't come from a human end user. These instances are called false positives.

For example, if you send a simulated phishing email to an employee, a real-time threat detection solution may scan and 'click' on the link in the email and mislead you to believe that the user did.

False positives can influence how your organization's phishing simulation reporting data is interpreted and, eventually, lead to unsubstantiated insights fuelling your overall training program strategy.

Why Causes Bot-Clicks?

While most bot-clicks are down to third-party security solutions, there are many reasons why they occur. One of the most common is where an employee will spot a simulated phishing email and then use the "Mark as Phishing" feature using a phishing report button, an add-in obtainable in Outlook and other email clients. Doing so will prompt the email provider to scan the link for malicious content.

Another common scenario is that a user will scan an email or attachment with a third-party security service , such as Microsoft Safelink, to check the attachment is secure, which will again probe the link. This sequence of actions will result in a bot click that causes a phishing false positive bot click.

Other reasons why bot clicks occur include:

- Endpoint security and antivirus software scanning links
- Mobile devices previewing link content
- Users forward emails to other users prompting the mail server to scan the email
- Poorly configured spam filter allowlisting scanning links

Why Is Spotting Bot-Clicks Important?

The most significant problem raised by bot-clicks is that they decrease the accuracy of the phishing simulation and make it harder to gauge employees' security awareness. If bot-clicks artificially inflate the number of users failing phishing simulations, then this can indicate that your training was ineffective when those were bot clicks.

In short, bot-clicks are a problem because they increase false positives, reduce the overall accuracy of the phishing simulation and make it hard to monitor or record employee performance during tests.

At the same time, being prepared to address false positives increases the effectiveness of your phishing simulations as you'll be able to gather more accurate data that determines how effective employees are at spotting phishing emails.

How to Spot False Positives?

Two of the easiest ways to tell if your phishing simulation is affected by false positives is if you see an unusually high click rate or a high volume of external IP addresses. These indicate that a remote security solution scanned your links multiple times.

Also, looking up those IPs to see who they belong to will often provide information around the corresponding tool. For example, Microsoft Safelink would boast an IP address that refers back to Microsoft Azure.

Another sign is if an employee failed a test but claims they didn't click on any links. So if multiple employees are found to have failed tests but are adamant they didn't click on any email links, it's worth investing further.

You can also catch bot clicks by looking out for clicks made by operating systems and web browser versions. Often referred to as a "user agent," it's the combination of operating system and web browser that opens the URL. Using user agents as a cross-reference can help establish clicks that originate from outside your typical environment.

How to Prevent a Phishing False Positive?

You can prevent false positives by taking an inventory of all the software, security products, and services you're using throughout your environment, checking the documentation, and identifying if they use scanning, analysis, or probing to see if there is a way to deactivate these capabilities for specific IP addresses and/or domains.

For instance, if you have an email security solution that offers an allowlisting feature, you can prevent links to phishing websites from being scanned or clicked on by bots.

As a rule of thumb, it's a good idea to complete test campaigns before committing to a live simulation to check if your current configurations will generate false positives and adjust your allowlisting and filtering settings to ensure accurate results.

It's also important to let participants know that they should only report phishing emails through an approved mechanism rather than their email provider's default reporting function to avoid phishing false positive results.

Recap

Phishing false positives are inconvenient, but they're easy to mitigate with some preparation. Getting to know what tools in your environment use bot-clicks enables you to start allowlisting the links so that bot-clicks don't decrease the accuracy of your data.

This way, you can ensure that, when you complete a phishing simulation, you know which employees were prepared and those who need extra support to combat the latest threats.

Want to find out how phishing awareness training can help your team spot phishing emails? Contact us (https://terranovasecurity.com/contact-us/) today.

Free Phishing Benchmarking Data to Train Your Cyber Heroes

Drive effective behavior change and strengthen your security awareness training initiatives with in-depth benchmarking data and expert guidance.

READ THE FULL REPORT (https://terranovasecurity.com/gone-phishing-tournament/)

Share: