

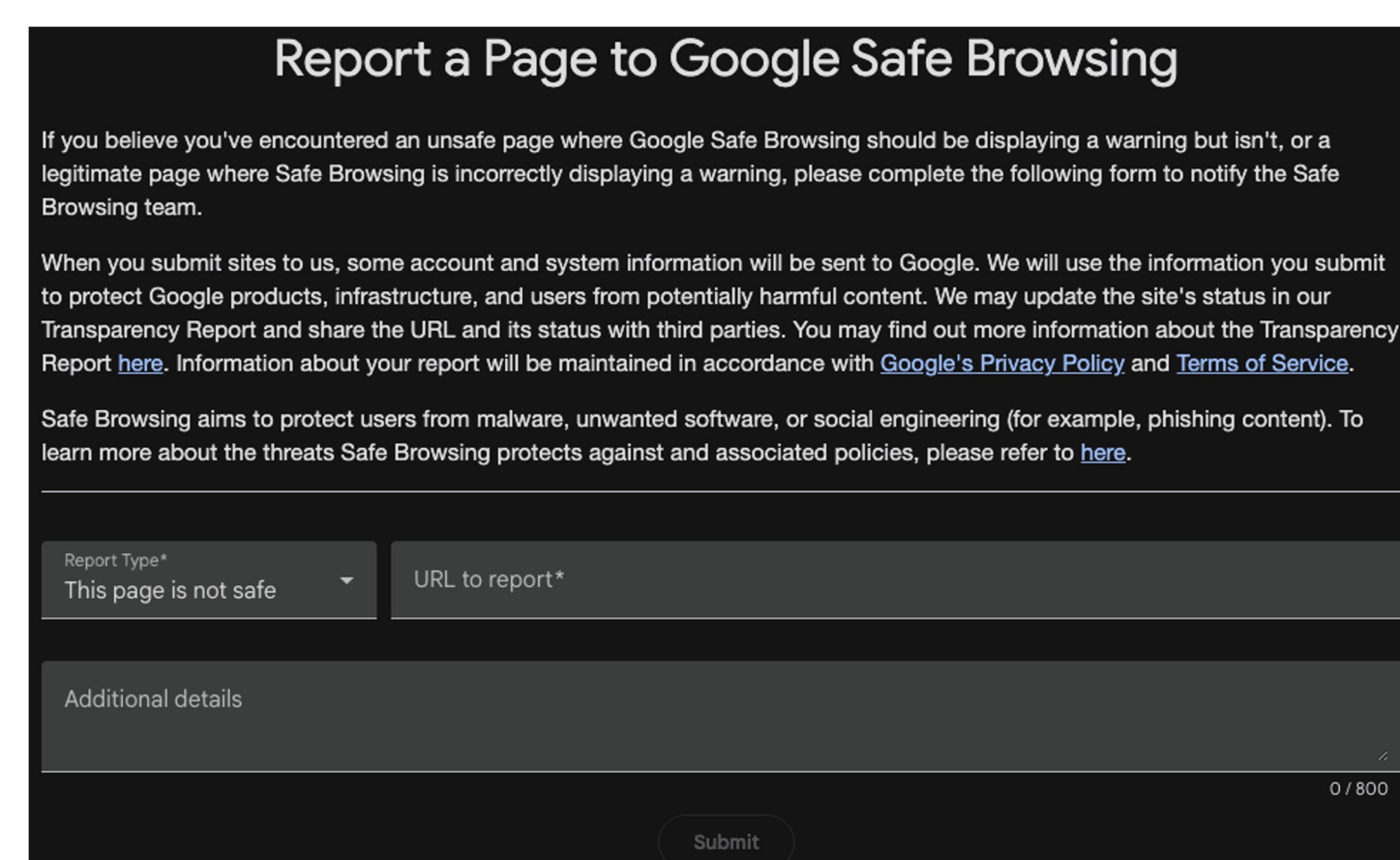
Doubly Dangerous: Evading Phishing Reporting Systems by Leveraging Email Tracking Techniques

Anish Chand, *Louisiana State University*
Nick Nikiforakis, *Stony Brook University*
Phani Vadrevu, *Louisiana State University*

Introduction

Attackers can repurpose email tracking techniques—traditionally viewed as a privacy risk—to evade email-based phishing detection systems. We show that major email providers' "Report phishing" workflows are fingerprintable via tracking vectors embedded in phishing emails, enabling attackers real-time cloaking of malicious content from security crawlers while still delivering payloads to human targets.

Prior Work

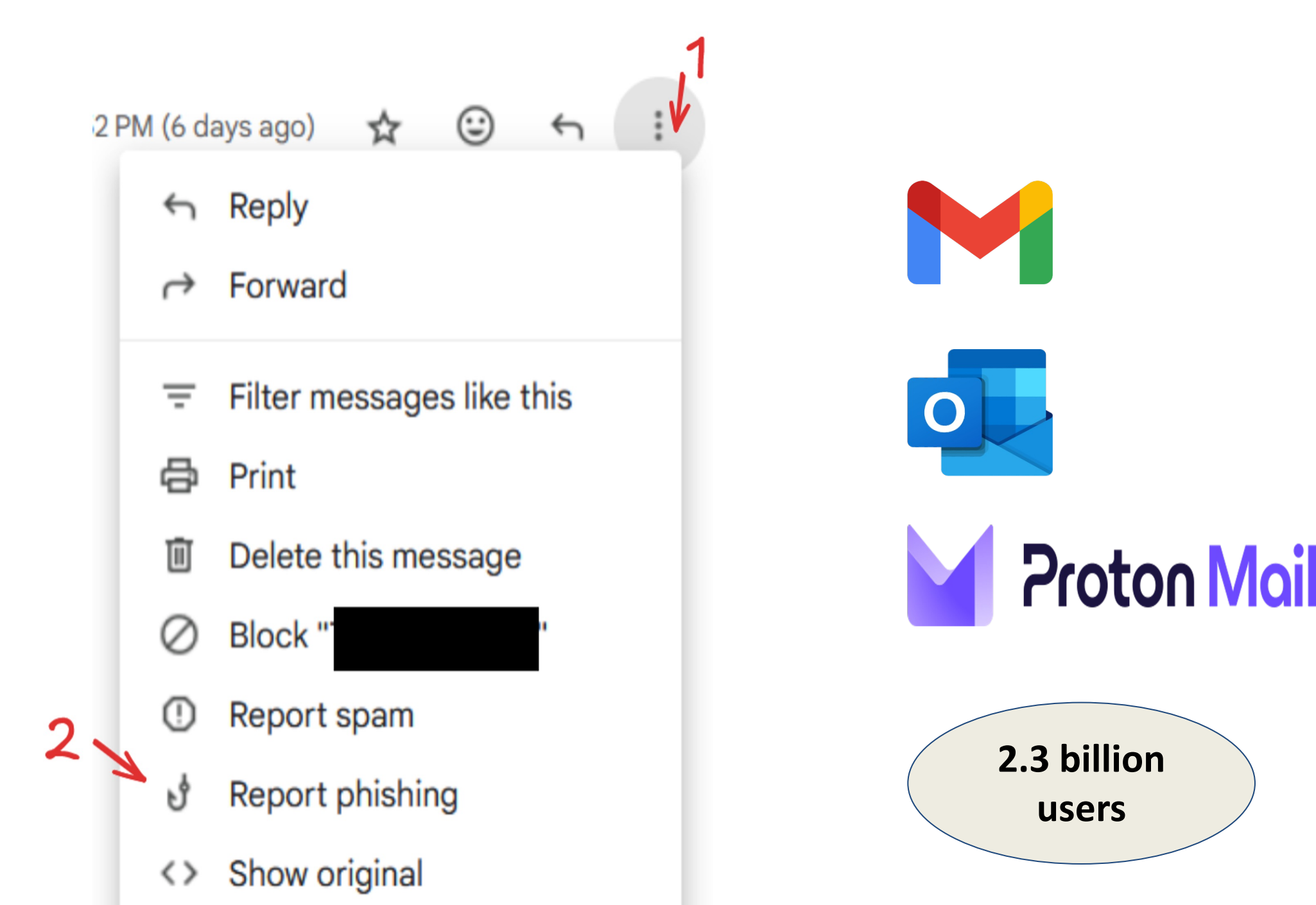


Phishfarm (SP '19), Phishtime (USENIX '20), CrawlPhish (SP '21), PhishPrint (USENIX '21), Acharya et al. (DIMVA '22)

not a widely popular reporting mechanism

Previous work have primarily studied phishing reporting systems with the primary reporting mechanism being web portal which everyday web users are not familiar with and unlikely to use

Our Focus



Everyday users are more familiar with the *built-in report phishing* button in their email. However, these reporting systems have not been studied before. Our work addresses this gap.

Methodology

We reported emails to email services. Each email was embedded with several curated HTML tags and CSS properties as tracking vectors.

Findings

1. **ALL** evaluated email providers process emails in three stages where the email tracking vectors get triggered.



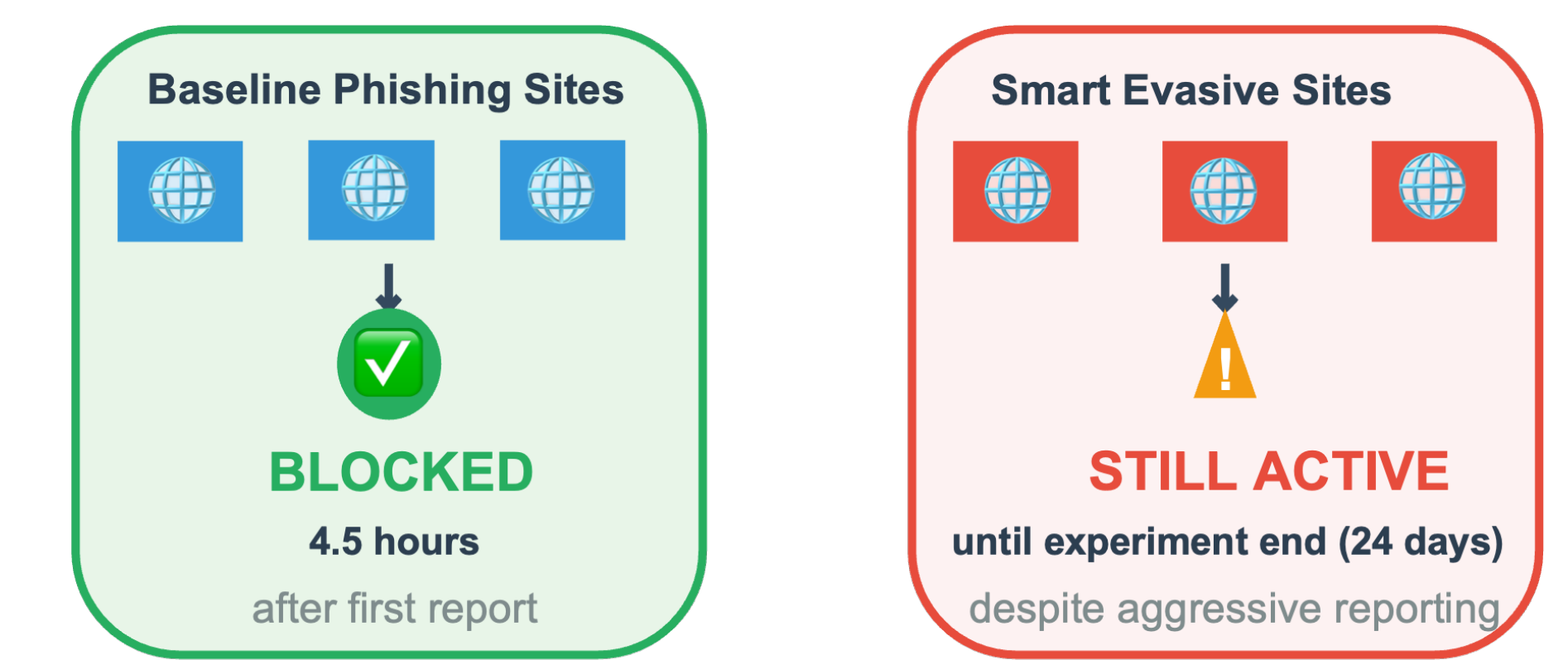
2. **ALL** email handlers of all evaluated email providers are **fingerprintable**.

Discernible Tracking Patterns

Identifiable HTTP headers	Identifiable tracking vectors
(e.g., Gmail-content-sampling)	(e.g., font, svg)

Simulation of an end-to-end attack

The phishing sites—powered by intelligence from email tracking vectors—were able to serve malicious content to victims while appearing benign to email service crawlers, remaining undetected throughout the lifespan of the experiment compared to baseline sites which were blocked in the matter of hours.



Highly evasive attack in practice.

Suggested Countermeasures:

- Disable remote object loading after email reports
- Homogenize headers and network behavior across all email stages
- Suppress or randomize "email open" signals

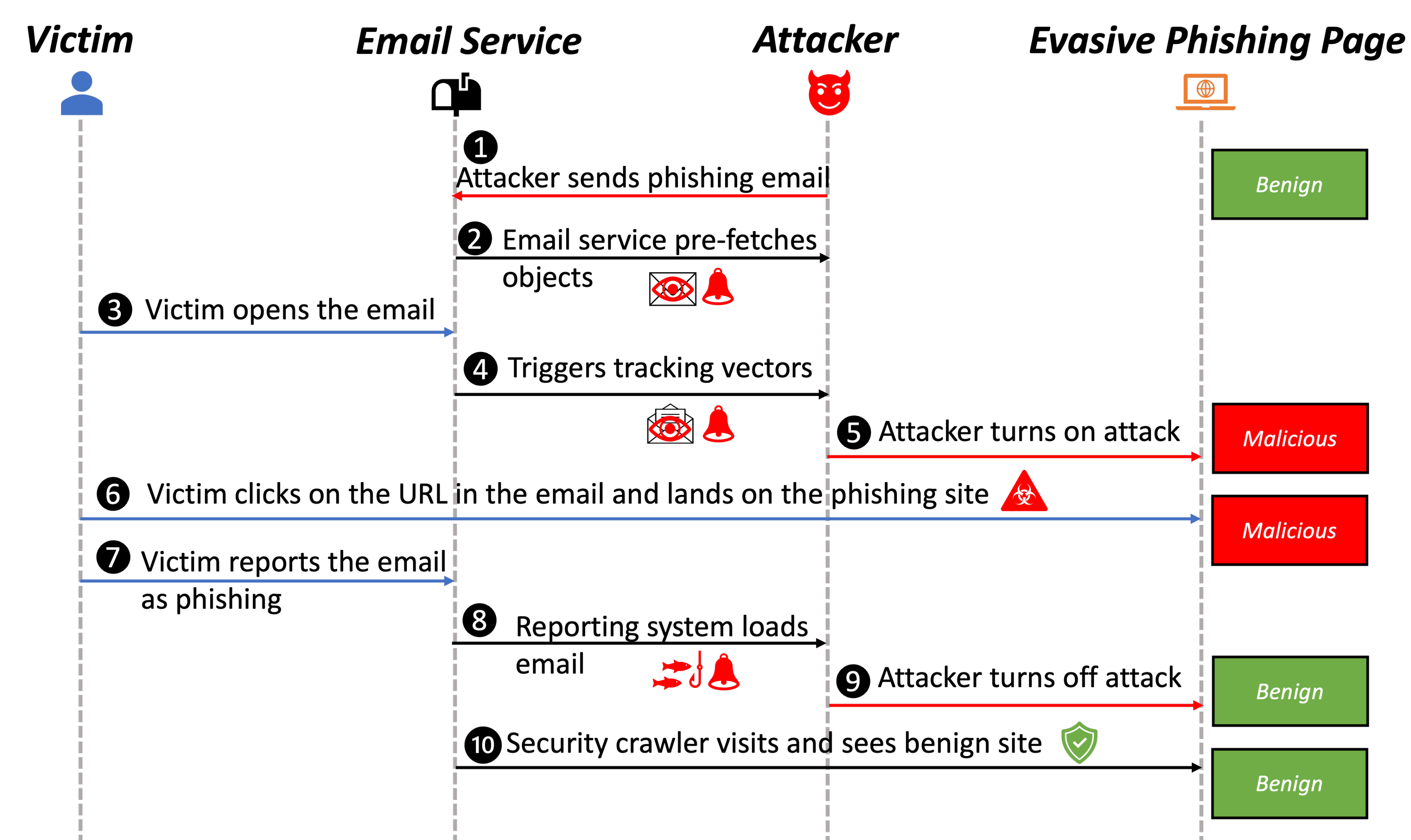
Impacts:

- Received a vulnerability reward from Google
- Our countermeasures got adopted by some email providers

Email tracking is **doubly dangerous**

It not only poses serious privacy risks **but also carries serious security implications.**

Attack Model



The attack model illustrates a scenario of an evasive phishing attack in which the victim recognizes the attack and reports it. Due to the attacker's ability to fingerprint different stages of email processing, they can evade the email service's security crawlers using email tracking and cloaking.

Paper here



Artifacts here

