



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

Authors: Anish Chand, Nick Nikiforakis, and Phani Vadrevu



Prior Work

Report a Page to Google Safe Browsing

If you believe you've encountered an unsafe page where Google Safe Browsing should be displaying a warning but isn't, or a legitimate page where Safe Browsing is incorrectly displaying a warning, please complete the following form to notify the Safe Browsing team.

When you submit sites to us, some account and system information will be sent to Google. We will use the information you submit to protect Google products, infrastructure, and users from potentially harmful content. We may update the site's status in our Transparency Report and share the URL and its status with third parties. You may find out more information about the Transparency Report [here](#). Information about your report will be maintained in accordance with [Google's Privacy Policy](#) and [Terms of Service](#).

Safe Browsing aims to protect users from malware, unwanted software, or social engineering (for example, phishing content). To learn more about the threats Safe Browsing protects against and associated policies, please refer to [here](#).

Report Type*
This page is not safe ▼

URL to report*

Additional details

0 / 800

Submit

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

**not a widely popular
reporting mechanism**

Prior Work

Report a Page to Google Safe Browsing

If you believe you've encountered an unsafe page where Google Safe Browsing should be displaying a warning but isn't, or a legitimate page where Safe Browsing is incorrectly displaying a warning, please complete the following form to notify the Safe Browsing team.

When you submit sites to us, some account and system information will be sent to Google. We will use the information you submit to protect Google products, infrastructure, and users from potentially harmful content. We may update the site's status in our Transparency Report and share the URL and its status with third parties. You may find out more information about the Transparency Report [here](#). Information about your report will be maintained in accordance with [Google's Privacy Policy](#) and [Terms of Service](#).

Safe Browsing aims to protect users from malware, unwanted software, or social engineering (for example, phishing content). To learn more about the threats Safe Browsing protects against and associated policies, please refer to [here](#).

Report Type*

This page is not safe

URL to report*

Additional details

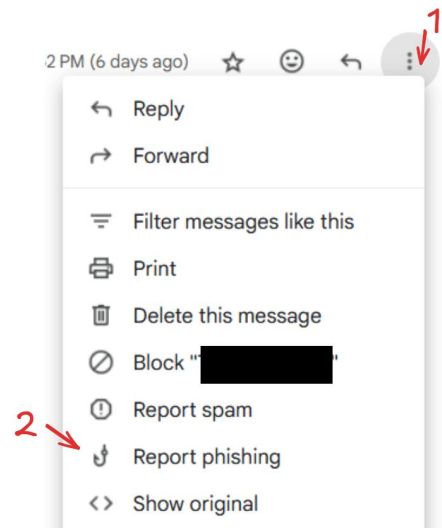
0 / 800

Submit

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

**not a widely popular
reporting mechanism**

Our focus



Proton Mail

**2.3 billion
users**

Q1 How do email services handle email phishing reports?

Q1 How do email services handle email phishing reports?

ALL evaluated email providers process emails in three stages.



Q1 How do email services handle email phishing reports?

ALL evaluated email providers process emails in three stages.



Q2 Are these email handlers vulnerable to tracking/fingerprinting?

Q1 How do email services handle email phishing reports?

ALL evaluated email providers process emails in three stages.



Q2 Are these email handlers vulnerable to tracking/fingerprinting?

Discernible Tracking Patterns

Identifiable HTTP headers

(e.g., Gmail-content-sampling)

Identifiable tracking vectors

(e.g., font, svg)

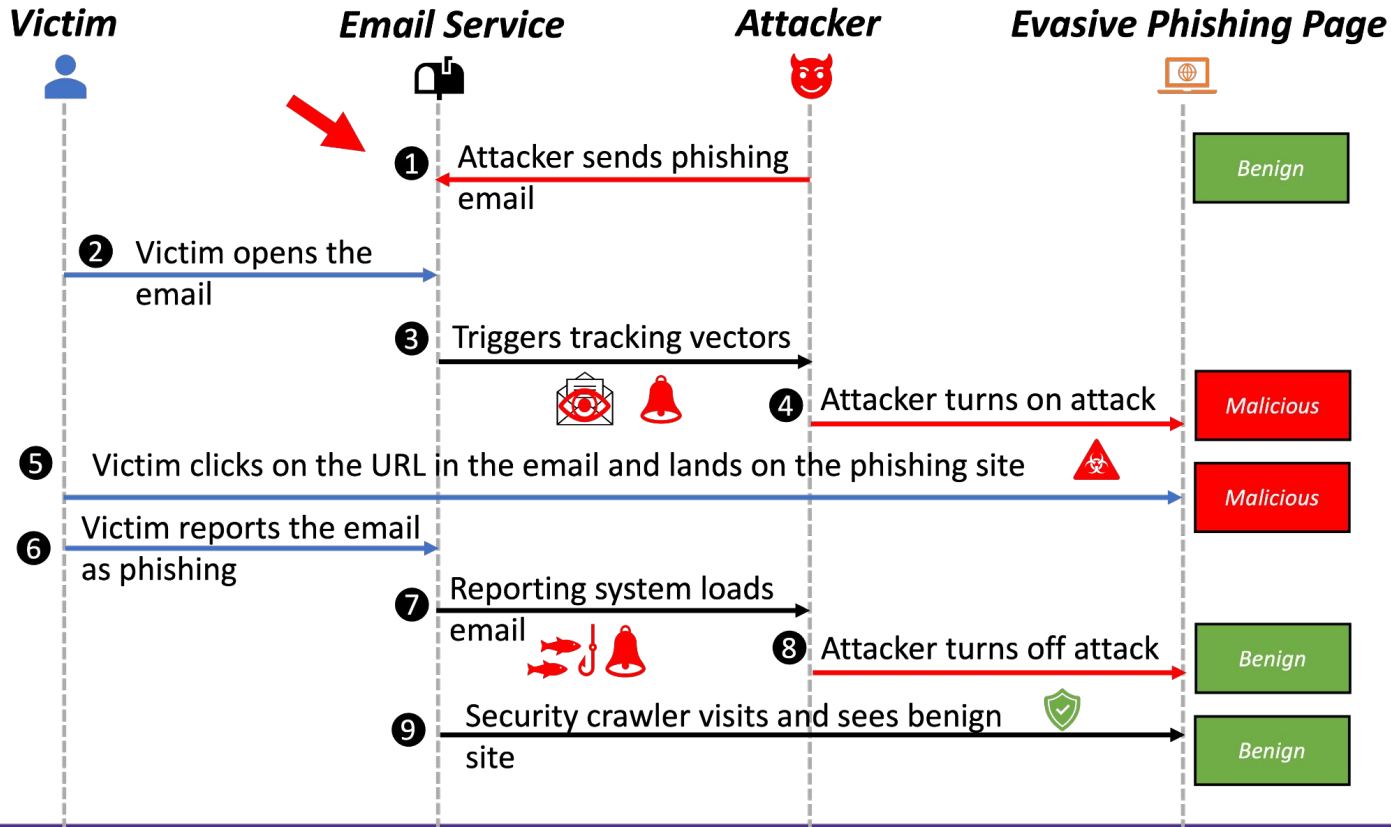
YES. ALL email handlers of all evaluated email providers are fingerprintable.

Q3

How can an attacker exploit the fingerprintability of email reporting systems to launch evasive phishing campaigns?

Q3

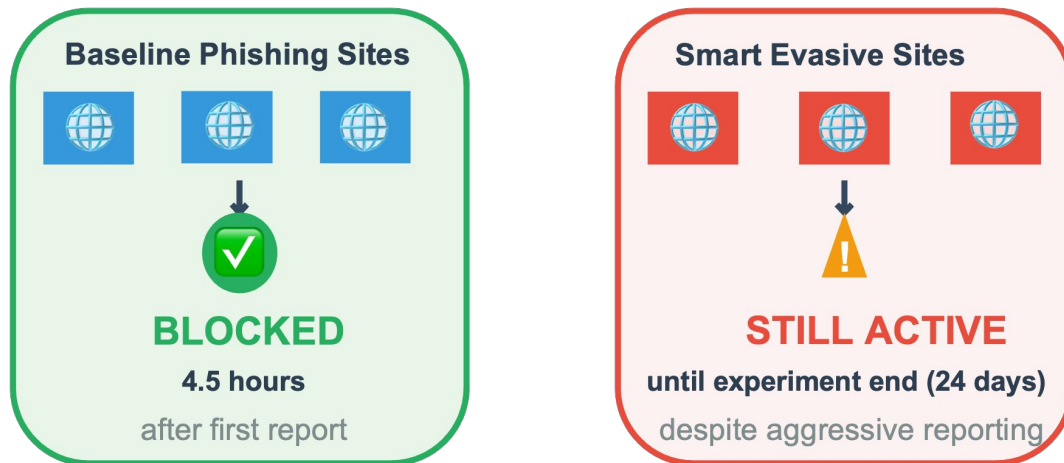
How can an attacker exploit the fingerprintability of email reporting systems to launch evasive phishing campaigns?



Q4 How effective is the resulting evasion attack in practice?

Q4 How effective is the resulting evasion attack in practice?

Simulated phishing experiment



Highly evasive attack in practice.

Email tracking is indeed *doubly dangerous*

Suggested Countermeasures:

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

Impact:

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



Artifacts available at
Zenodo



achan41@lsu.edu