Phishing Landscape 2022
An Annual Study of the Scope and Distribution of Phishing

by
Greg Aaron
Lyman Chapin
David Piscitello
Dr. Colin Strutt
Interisle Consulting Group, LLC

19 July 2022
Executive Summary

Phishing remains a significant threat to millions of Internet users. Phishing attacks lure victims to a website that appears to be run by a trusted entity, such as a bank or a merchant. The website, however, is a deception, and the site’s content is designed to persuade a victim to provide sensitive information.

Our goal in this study was to capture and analyze a large set of information about phishing attacks, to better understand how much phishing is taking place and where it is taking place, and to see if the data suggests better ways to fight phishing. To do so we determined when attacks occur and how quickly phishers act. We studied where phishers get the resources that they need to perpetrate their crimes — such as where they obtain domain names, and what web hosting is used. This analysis can identify where additional phishing detection and mitigation efforts are needed and can identify vulnerable providers. We also report on the wide range of brands targeted by phishers, and how often they take advantage of the unique properties of internationalized domain names (IDNs).

To assemble a deep and reliable set of data, we collected over three million phishing reports from 1 May 2021 to 30 April 2022 from four widely used and respected threat intelligence providers: the Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus. From that data we identified 1,122,579 unique phishing attacks.

For this 2022 landscape study, we also analyzed phishing reports collected over a two-year period, a total of nearly five million phishing reports collected from 1 May 2020 to 30 April 2022. By adding biennial measurements and analyses, we began to consider questions like, “How do the yearly trends for phishing attacks, domain names used for phishing, etc., compare to biennial trends?” and “Are phishers “doing business” at the same registry, registration, or hosting services year after year?”

Our yearly and now, biennial, studies illustrate that phishing is a highly profitable, constantly evolving and expanding industry. Phishing leverages Internet resources, exploits vulnerable technologies, and takes advantage of policy and legislative regimes that are siloed and, by our measurements and analyses, ineffective. From our studies, we observe that

- **Silos frustrate phishing response:** The naming, addressing, and hosting ecosystem exploited by phishers (and cyberattackers generally) is encumbered by vertically isolated (“silod”) policy and mitigation regimes.

- **Registrars, registries, and hosting providers can take action:** Registries and registrars should identify, “lock”, and suspend domains reported for phishing, and hosting and cloud service providers should remove phishing content or shut down accounts where phishing occurs; all parties should be more responsive to abuse complaints, especially for cybercrimes such as phishing, but they must begin to do so in a more coordinated and determined manner.

- **Regulation and legislation could help:** Changes to or introduction of policy or regulation may be necessary to effectively mitigate phishing. Obliging operators to validate the identity of users and customers, coupled with agreement on a common definition of lawful access that acknowledges the role that the private sector plays in combatting cybercrime, could reduce both the incidence of phishing and the difficulty of responding to it.
## Findings

**1,122,579 phishing attacks**

A 61% increase over the previous yearly study  
Monthly reported phishing attacks more than doubled since May 2021

**853,987 domain names reported for phishing**

A 72% increase over the 2021 study

**588,321 malicious domain name registrations**

Domains registered by phishers for phishing attacks  
increased 83% over 2021 study

**New gTLDs domains used disproportionately for phishing**

34% of phishing domains in .COM and .NET  
ccTLDs run by Freenom represent 40% of all ccTLD phishing domains

**US hosting networks attract phishers**

86% of phishing attacks reported against the top 10  
hosting networks are using IP addresses in the US

**Phishers are targeting more brands**

Meta Platforms (Facebook, WhatsApp), Amazon,  
Microsoft (Outlook), and Apple

**257% increase in cryptocurrency phishing**

Wallet brands most targeted  
79% of gTLD cryptocurrency phishing domains  
were maliciously registered

**13% of all phishing attacks used subdomain services**

82% hosted on domains operated by  
top ten subdomain service providers