netskope

Cloud and Threat Report: Phishing

From Fake Websites to Impersonated Cloud Apps

BROUGHT TO YOU BY

netskope
THREAT LABS

EXECUTIVE SUMMARY

In this edition of the Cloud Threat Report, we highlight current phishing attack trends and how they are starting to change based on cloud app usage. We take a closer look at two types of phishing:

- Users lured by fake login pages that capture usernames, passwords, and MFA codes
- Users tricked by fake third-party cloud apps into authorizing access to their cloud data and resources

An average of 8 out of every 1,000 enterprise users clicked on a phishing link or otherwise attempted to access phishing content in Q3 2022. Most industries exhibited similar phishing rates, with the exception of Financial Services, with only 5 out of 1,000 users accessing phishing content. Geographically, most regions also were close to the average, although the Middle East had nearly twice the incidence of users accessing phishing content.

While email remains a common mechanism for delivering phishing attacks, it is overshadowed by the use of other channels, including search engines, social media, and personal blog sites. Popular cloud applications such as Google Docs and Microsoft OneDrive are also increasingly used to phish users.

An early trend shows that credential attacks are starting to leverage third-party app access using OAuth application approvals. Third-party application access is ubiquitous, and phishing threats are starting to target the large attack surface offered by these third-party access relationships.

Organizations can implement anti-phishing controls including secure web gateways, train users, and ensure that new attack paths such as OAuth approvals are restricted or locked down. In addition, controls to manage compromised credentials can be implemented including multi-factor authentication (MFA), IP/device access policies, and behavioral detection.

REPORT HIGHLIGHTS

Fake Login Pages

- An average of 8 out of 1,000 users access phishing sites and content.
- 22% of phishing content is hosted by Content Servers, followed by 17% using newly registered domains.
- Personal sites and blogs account for 26% of referrals to phishing content, followed by webmail at 11% and search engines at 6%.

Third-party Apps

- Organizations on average granted more than 440 third-party applications access to their Google data and applications.
- More than 44% of third-party applications accessing Google Drive have access to either sensitive data or all data on the user’s Google Drive.

ABOUT THIS REPORT

Netskope provides threat and data protection to millions of users worldwide. Information presented in this report is based on anonymized usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers with prior authorization. This report contains information about phishing detections raised by Netskope's Next Generation Secure Web Gateway (Next Gen SWG), not considering the significance of the impact of each individual threat. Stats in this report are based on the three month period from July 1, 2022 through September 30, 2022. Stats are a reflection of both user behavior and attacker techniques.

Netskope Threat Labs

Staffed by the industry's foremost cloud threat and malware researchers, Netskope Threat Labs discovers, analyzes, and designs defenses against the latest cloud and data threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DEF CON, Black Hat, and RSA.

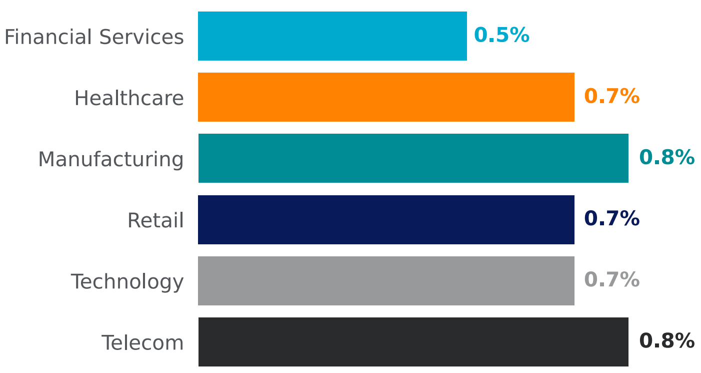
Who does phishing affect?

The Anti-Phishing Working Group (APWG) reports that phishing attacks continue to rise to record levels, with financial institutions, cloud apps, and social media accounting for more than half of all phishing targets. This Cloud and Threat report explores the phishing attacks that are successfully reaching enterprise users. In Q3 2022, 8 out of every 1,000 enterprise users clicked on a phishing link or otherwise attempted to access phishing content.

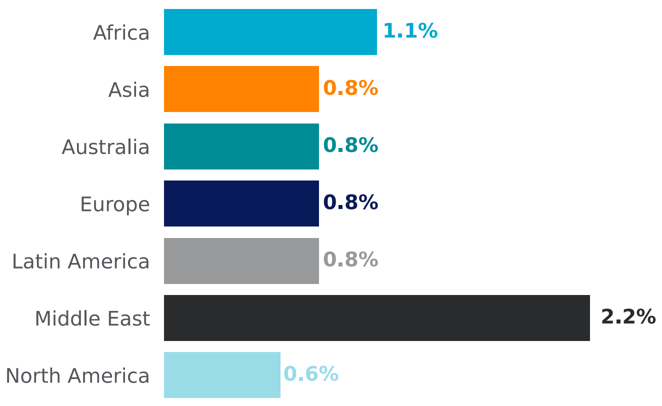
Among industry verticals, Financial Services stands out as having the lowest percentage of users accessing phishing content. At 5 out of 1,000, the phishing rate in Financial Services is less than two-thirds the average. Contributing to this lower-than-average phishing rate in financial services is the use of stricter policies and controls, including more restrictive URL filtering policies and use of technologies like remote browser isolation (RBI).

Regionally, Africa and the Middle East stand out as the two regions with the highest percentages of users accessing phishing content. In Africa, the percentage of users accessing phishing content is more than 33% above average, and in the Middle East, it is more than twice the average. Attackers frequently use fear, uncertainty, and doubt (FUD) to design phishing lures and also try to capitalize on major news items. Especially in the Middle East, attackers appear to be having success designing lures that capitalize on political, social, and economic issues affecting the region.

Phishing by Industry



Phishing by Region



Where is phishing content hosted?

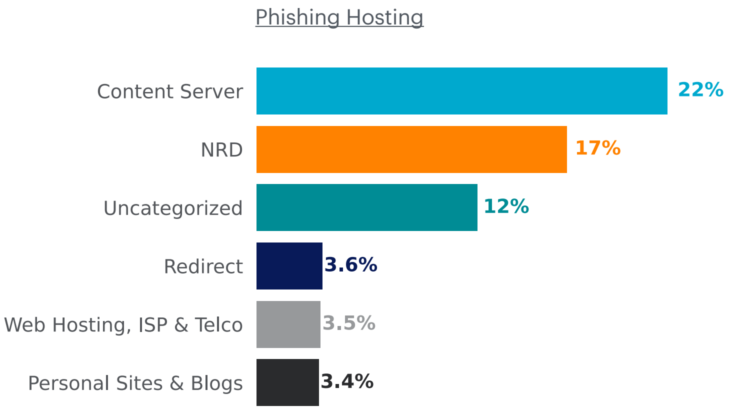
Traditionally, phishing attacks have involved fake websites designed to mimic legitimate login pages, especially those of financial institutions, cloud apps, and social media sites. This section explores where attackers are hosting these websites, highlighting a trend away from custom domains and toward shared hosting providers and cloud services.

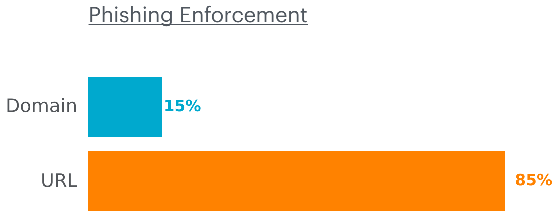
The largest fraction of phishing content reaching users, 22%, comes from content servers. Content servers include popular content delivery networks (CDNs), used to deliver a variety of legitimate web content. Free hosting services are also commonly abused by attackers, with Blogger, Weebly, Google Sites, Azure Web Apps, and Amazon S3 among the apps where attackers had the most success in reaching their victims in Q3. One recent cryptocurrency phish used an initial page in Google Sites with additional links to a login page hosted in Azure—a form of redirection using two different free hosting services.

Using custom domains to host phishing sites remains a popular tactic, with 17% of phishing content that users visited hosted on newly registered domains (NRDs) and 12% hosted on uncategorized domains. Custom domains offer attackers the ability to craft URLs that closely resemble the legitimate domains they are mimicking, making them harder for victims to recognize, but often easier for security software to filter out.

Redirection services, such as URL shorteners, are a popular tool used in phishing because they can obfuscate the true target of a hyperlink and provide some resilience: If the target link is taken down, attackers can update the redirector to point to a new link. This is especially important for phishing content because it is usually short-lived.

Overall, the majority of the phishing content reaching users is not hosted on custom domains, but rather on shared hosting services and content servers. As a result, only 15% of the phishing content Netskope blocked in Q3 was blocked by domain, with the other 85% blocked at the URL level.





How are users lured into clicking on phishing links?

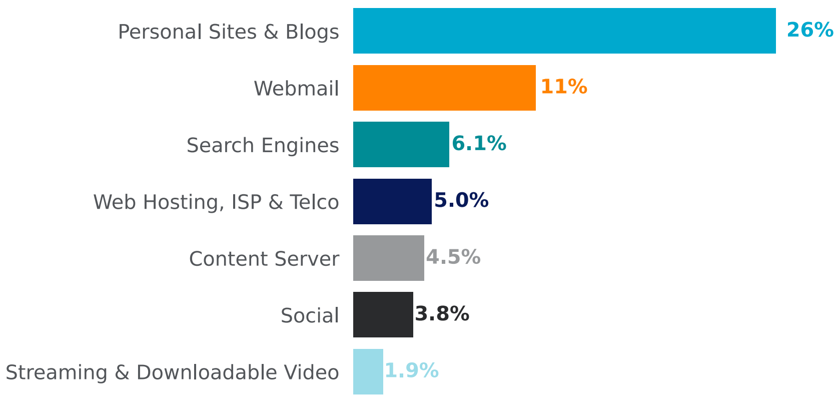
The referrer URLs for phishing alerts generated by the Netskope Security Cloud platform provide clues about how users are being lured into clicking on phishing links. While email is typically considered the top phishing threat, only 11% of the phishing alerts in Q3 2022 were referred from webmail sites.

Instead, personal sites and blogs, particularly ones hosted on free hosting services, were the most common referrers to phishing content. There were two primary types of referrals, ones from spam on legitimate sites and blogs, and ones from sites and blogs that were created specifically to promote phishing content.

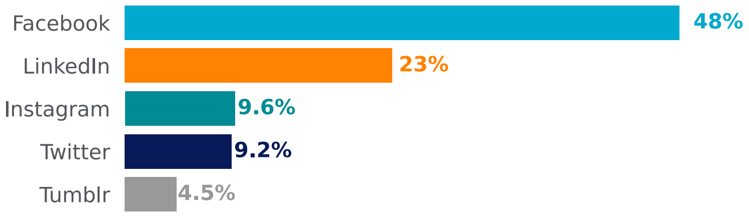
Other popular referrers include social media sites and streaming video sites (namely YouTube) where attackers post videos, pictures, and comments to bait victims into visiting phishing sites.

Search engine referrals are also common, mostly from Google and Bing, reflecting primarily search engine market share. Attackers are weaponizing data voids by creating pages centered around uncommon search terms where they can establish themselves as one of the top results for those terms. Use of this technique appears to be widespread and automated, with thousands of pages sharing similar templates spanning thousands of topics in many different languages. Topics include how to use specific features in popular software such as SAP and SPSS, quiz answers for online courses, manuals for a variety of different business and personal products, and personal finance questions.

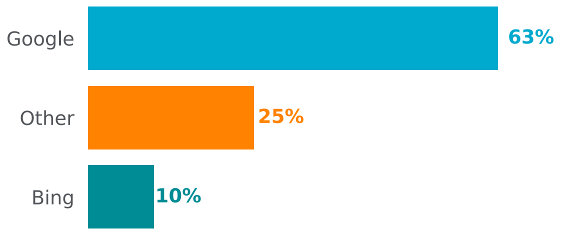
Phishing Referers



Social Media Phishing Referers



Search Engine Phishing Referers



Do all phishing attacks use fake login pages?

Phishing attacks often use fake login pages but there is a growing shift to phishing that abuses cloud applications, where attackers focus on:

- Creating fake cloud applications that are OAuth-enabled
- Tricking users into granting access to those fake applications
- Using OAuth access tokens and APIs to access users' cloud data and resources

Targeting cloud applications provides several advantages for attackers:

- **Large attack surface:** OAuth has been adopted by Microsoft and Google, SSO vendors and nearly all SaaS vendors.
- **Bypassing multi-factor authentication (MFA):** Stealing OAuth tokens provides access to the user's data without needing to go through MFA.
- **Permanent access:** Access can be refreshed almost indefinitely without need for reauthentication.
- **Defensive challenges:** Security controls for prevention, detection, and remediation of OAuth credential theft are lagging.

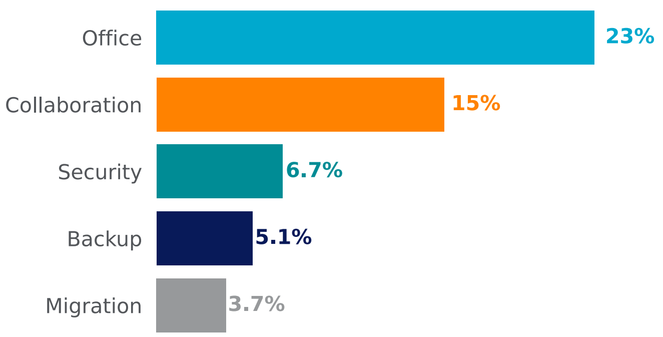
The most popular types of third-party apps authorized by users include Office, Collaboration, and Security apps. Attackers have already created fake apps mimicking legitimate apps in these categories, and we expect the number of fake apps to increase in the coming months.

440 third-party applications on average were granted access by organizations to their Google resources.

12,330 different applications were authorized by users in one organization.

82% of organizations with at least 500 users, granted access to at least 250 different cloud applications.

Third Party App Categories



What can attackers access with fake third-party cloud apps?

Third-party app ecosystems allow the third-party to request permissions to access information in the primary app. In this section, we use Google Workspace as a case study to illustrate the types of permissions third-party apps typically request.

Users are accustomed to granting third-parties access to their data, commonly granting permissions to third-party applications to read/write GMail, Google Sheets, Google Drive, or their contacts.

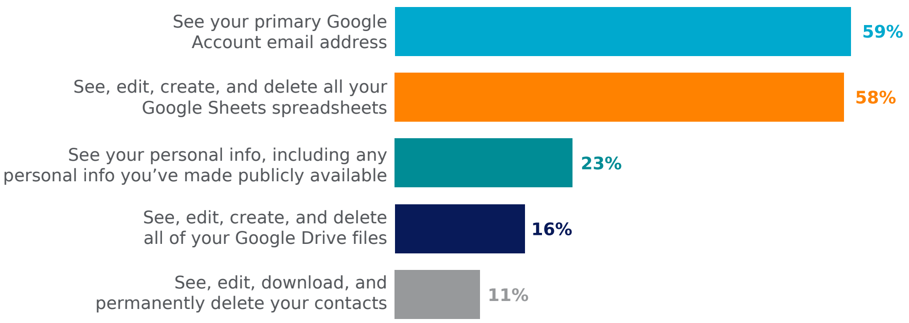
Attackers have capitalized on this trend of third-party app authorization to help their social engineering efforts, creating fake apps that mimic legitimate apps and request similar permissions.

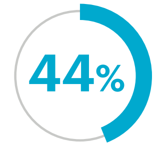
An app that requests email access can be used as a form of business email compromise. An app that requests data access can be used to steal sensitive data, sabotage victim environments, or target other users.

One way attackers have weaponized third-party apps is by creating fake OAuth apps in a type of attack called an illicit consent grant.

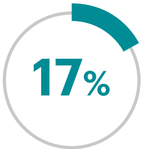
Attackers can also compromise apps that provide legitimate functionality such as the CamScanner application, which provides document scanning but can be used to access sensitive data.

Third Party App Scopes



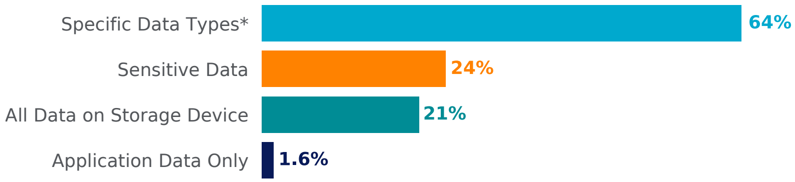


of applications request permission to access either sensitive, private data or all data on the user's Google Drive.



of applications request write permission on all data on a user's Google Drive.

Third Party App Scopes Categories



* Specific Data Types refers to all data of a specific type e.g. all Google Spreadsheets or all Docs.

RECOMMENDATIONS

To protect against evolving phishing attacks, Netskope recommends taking the following procedures:

1 Lock down cloud application access to your data by using Cloud and SaaS Security Posture Management (CSPM and SSPM) to ensure that all cloud apps that process or store sensitive data are appropriately locked down to protect such data from accidental or unauthorized exposure.

2 Reduce browsing risk for newly registered domains, newly observed domains, uncategorized websites, and other security risk categories by using Remote Browser Isolation (RBI).

3 Use available vendor controls related to third-party application access including OAuth session timeouts, restricting of OAuth application approvals to administrators, and implementing a sanctioned or approved application list. Enforce these control settings with a CSPM or SSPM solution.

4 Detect and block phishing attacks by deploying a security service edge (SSE) cloud platform with a secure web gateway (SWG) to not only block sites hosting phishing content but also suspicious referring domains e.g. non-standard search, job, or ad sites.

5 Invoke real-time coaching to users by using alerts, warning users of suspicious or suspected phishing websites.

6 Mitigate stolen credentials by enabling multi-factor authentication (MFA) and extend MFA to unmanaged apps via your identity service provider or SSE platform.

7 Use single sign-on (SSO) for managed apps to maintain centralized access control over access to sensitive data and ensure that policies can be applied to authentication and authorization activities through the use of SSO proxies (SAML Proxy) and inline security filters.

8 Use behavioral analytics to detect activity from both compromised passwords as well as compromised tokens such as OAuth.

9 Enable zero trust principles for least privilege access to data with continuous monitoring from rich contextual analytics and reporting.

LEARN MORE

For more information on cloud-enabled threats and our latest findings from Netskope Threat Labs, go to:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

For more information on how to mitigate risk, contact us today:
WWW.NETSKOPE.COM/REQUEST-DEMO

BROUGHT TO YOU BY

netskope
THREAT LABS