Netskope Threat Labs: Phishing Clicks Nearly Tripled in 2024, Ubiquitous Use of Personal Cloud Apps and GenAI Tools Require Modern Workplace Security to Mitigate Risk

January 6, 2025

New research details rising enterprise cloud security risks, successful strategies adopted to manage genAI risks in 2024

SANTA CLARA, Calif. – January 7, 2025 – Netskope, a global leader in Secure Access Service Edge (SASE), today shared new research showing that, as a result of the growing prevalence and sophistication of phishing attacks, enterprise employees click on phishing lures nearly three times more in 2024 compared to the prior year. The findings, based on data gathered by Netskope from enterprises worldwide, and published as part of Netskope's annual Cloud & Threat Report , reveal growing security risks related to the persistent use of personal cloud apps and continued adoption of genAI tools in the workplace, underscoring the need to adopt modern data security to proactively manage that risk.

Phishing lures triple in success rate

Despite organizations' repeated attempts at security awareness training, with a particular emphasis on how employees can avoid being phished, in 2024 enterprise users clicked on phishing lures at a rate nearly three times higher than in 2023. More than eight out of every 1,000 users clicked on a phishing link each month – up 190% from last year when fewer than three per thousand enterprise users fell prey to phishing attempts.

Where attackers host their malicious payloads is also an element of social engineering. Attackers want to host malicious content on platforms where victims place some implicit trust, including popular cloud apps such as GitHub, Microsoft OneDrive, and Google Drive. In 2024, downloads of malicious content from popular cloud apps occurred in 88% of organizations at least once per month.

The top target for phishing campaigns that users clicked on in 2024 were cloud applications, representing more than a quarter of all phishing clicks at 27%. Among the cloud apps, Microsoft was by far the most targeted brand at a rate of 42% where attackers targeted Microsoft Live and Microsoft 365 credentials.

Personal apps blurring the lines

The ubiquity of personal cloud apps in the enterprise has created an environment where employees are knowingly or unknowingly using these apps to process or store sensitive information, leading to loss of organizational control over data and potential data breaches. Among the top personal apps that users send data to are cloud storage, webmail, genAI, social media, and personal calendar apps.

In 2024, 88% of all employees used personal cloud apps each month, with more than one out of every four users (26%) uploading, posting, or otherwise sending data to personal apps. Sensitive data being leaked through personal apps is top of mind for most organizations, with the most common type of data policy violation being for regulated data (60%), which included personal, financial, or healthcare data being uploaded to personal apps. The other types of data involved in policy violations include intellectual property (16%), source code (13%), passwords and keys (11%), and encrypted data (1%).

GenAI growth trends continue

In 2023, genAI came roaring into the workplace, and growing adoption of genAI apps by both organizations and users—as well as the overall volume of genAI apps in use— continued through 2024. Specifically:

- Organizational use grew from 81% of companies using genAI apps in 2023 to 94% in 2024. ChatGPT continues to be the most popular genAI app, being used in 84% of organizations.
- Employee use rate of genAI apps tripled from 2.6% of all people in organizations to 7.8%. Retail and technology organizations lead all industries with an average of more than 13% of all employees using genAI apps monthly.
- Organizations now use an average of 9.6 genAI apps, up from 7.6 a year ago. The top 25% of organizations now use at least 24 genAI apps, whereas the bottom 25% are using 4 genAI apps at most.

Managing the genAI data risk

As genAI apps continued to solidify their standing as an enterprise mainstay (94% of organizations now use them) in 2024, organizations have shown they are still in the early stages of putting controls in place for the safe enablement of genAI and to help mitigate the data risks posed by genAI apps:

- 45% of organizations use DLP to control the flow of data into genAI apps. Industry adoption of DLP for genAI varies widely with telecommunications the highest at 64%.

- 34% of organizations use real-time interactive user coaching to empower individuals to make appropriate and informed decisions.
- 73% of the time, when prompted with warnings of a potential company violation, users opt to not proceed based on coaching information provided.
- 73% of organizations block at least one genAI app, with a steady rate of 2.4 genAI apps blocked on average year over year.
- The number of apps blocked by the top 25% of all organizations blocking genAI apps has more than doubled from 6.3 apps to 14.6 over the past year.

Key takeaways for organizations

Netskope recommends organizations take the following steps to protect their environments:

- Users are being bombarded with phishing links from all directions: email, social media, ads in search engine results, and all over the web. Furthermore, genAI is making it easier for attackers to craft convincing phishes. All of this underscores that relying on education alone to help users detect a phishing attempt is insufficient and must be coupled with investments in modern data protection.
- Employees will continue to accidentally (or intentionally) share files via their personal accounts, include proprietary information in their personal backups, and use personal app instances to take data when leaving the organization. Regardless of intent, organizations must limit access to only those apps that serve a legitimate business purpose, create a review and approval process for new apps and implement a continuous monitoring process that will alert security operators when apps are being misused or have been compromised.
- The trajectory of more organizations and more employees using genAI will continue into 2025 as genAI becomes more entrenched in the workplace. At the same time, the number of genAI apps will continue to grow, necessitating controls to ensure that only approved apps are used, and only for approved use cases. Organizations should use modern data security to control data movement into approved apps, leverage real-time user coaching to empower people to make informed decisions when using genAI apps, and implement controls that block unapproved apps.

“The common thread for organizations working to safely enable the use of apps in the enterprise, and mitigate the challenges across the threat landscape, is the need for modern data security,” said Ray Canzanese, Director of Netskope Threat Labs. “Gone are the days when data security was an afterthought. It must be seamlessly integrated into every aspect of an organization’s operations. From defending against phishing to safeguarding personal apps and managing genAI, data security is no longer just a perimeter defense. It is a dynamic, proactive framework with real-time user coaching, DLP, and app-specific controls to stay ahead of an ever-changing threat landscape.”

Read the full *Cloud and Threat Report: 2025* here. For more information on cloud-enabled threats and the latest findings from Netskope Threat Labs, visit Netskope’s Threat Research Hub .

About Netskope

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, SaaS, web, and private application activity —providing security and accelerating performance without compromise.

Learn more at netskope.com, on the Netskope blog, on LinkedIn, and Instagram.

Media Contacts:

press@netskope.com