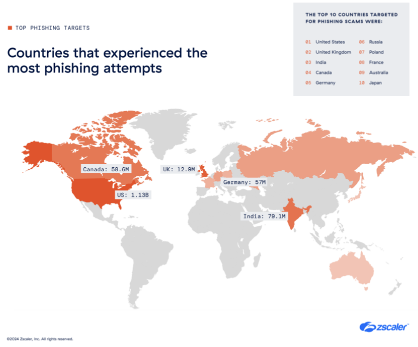
# Zscaler Research Finds 60% Increase in AI-Driven Phishing Attacks

April 23, 2024

**Annual ThreatLabz Phishing Report Unveils Rapidly Evolving Phishing Landscape, Underlining the Need to Adopt a Zero Trust Architecture**

- **Vishing (voice phishing) and deepfake phishing attacks are on the rise** as attackers leverage generative AI to amplify social engineering tactics.
- **The US, UK, India, Canada and Germany were the top five countries** targeted by phishing scams.
- **The finance and insurance industry faced 27.8% of overall phishing attacks**, the highest concentration among industries and a staggering 393% year-over-year increase.
- **Microsoft remains the most imitated brand, with 43.1%** of phishing attempts targeting it.

**Top Phishing Targets**



Top 10 countries that experienced the phishing attempts

SAN JOSE, Calif., April 23, 2024 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the release of the Zscaler ThreatLabz 2024 Phishing Report, which analyzes 2 billion blocked phishing transactions across the Zscaler Zero Trust Exchange™ platform, the world's largest cloud security platform, between January and December 2023. The data revealed a year-over-year increase of nearly 60% in global phishing attacks, fueled in part by the proliferation of generative AI-driven schemes such as voice phishing (vishing) and deepfake phishing. This year's report includes actionable insights on phishing activity and tactics, along with offering best practices and strategies to enhance an organization's security posture to prevent and minimize related threats.

"Phishing remains a persistent and often underestimated threat within the cybersecurity landscape, growing more sophisticated as threat actors harness cutting-edge advancements in generative AI and manipulate trusted platforms to intensify attacks," said Deepen Desai, CSO and Head of Security Research. "In this context, the latest ThreatLabz insights are more crucial than ever for informing our strategies and strengthening phishing defenses. These findings emphasize the need for organizations to adopt a proactive layered approach that integrates a robust zero trust architecture with advanced AI-powered phishing prevention controls to effectively counteract these evolving threats."

**North America experienced more than half of all phishing attacks, with EMEA and India following**

In 2023, the United States (55.9%), United Kingdom (5.6%) and India (3.9%) emerged as the top countries targeted by phishing scams. The high occurrence of phishing in the U.S. is attributable to its advanced digital infrastructure, large population of internet-connected users and extensive use of online financial transactions.

Canada (2.9%) and Germany (2.8%) rounded out the top five countries that experienced the most phishing attempts. The majority of phishing attacks originated from the U.S., the U.K., and Russia, while Australia entered the top 10 due to a 479% year-over-year surge in the volume of phishing content hosted in the country.

**Financial industry faces a nearly 400% increase in attacks**

The finance and insurance sector experienced the highest number of overall phishing attempts, amounting to a 393% increase of attacks from the previous year. Reliance on digital financial platforms provides ample opportunities for threat actors to carry out phishing campaigns and exploit vulnerabilities in this sector.

The manufacturing industry also experienced a significant uptick (31%) in phishing attacks from 2022 to 2023, underscoring the growing awareness of the industry's vulnerability. As manufacturing processes become more reliant on digital systems and interconnected technologies like IoT/OT, the risk of exploitation by threat actors seeking unauthorized access or disruption also grows.

**Microsoft remains the most impersonated brand used in phishing attacks**

ThreatLabz researchers identified enterprise brands such as Microsoft, OneDrive, Okta, Adobe and SharePoint as prime targets for impersonation due to their widespread usage and the value associated with acquiring user credentials for these platforms.

Microsoft (43%) emerged as the top imitated enterprise brand in 2023, with its OneDrive (12%) and SharePoint (3%) platforms also ranking in the top five—serving as lucrative targets for cybercriminals aiming to exploit Microsoft's vast user base.

**How a Zero Trust architecture can mitigate phishing attacks**

Organizations can implement a Zero Trust architecture with advanced AI-powered phishing prevention controls to effectively defend against the ever-evolving threat landscape highlighted in the report. The Zero Trust Exchange platform helps prevent conventional and AI-driven phishing attacks at multiple stages of the attack chain by:

- Preventing compromise: TLS/SSL inspection at scale, AI-powered browser isolation and policy-driven access controls

prevent access to suspicious websites.
- Eliminating lateral movement: Users connect directly to applications, not the network, while AI-powered app segmentation limits the blast radius of a potential incident.
- Shutting down compromised users and insider threats: Inline inspection prevents private application exploit attempts, and integrated deception capabilities detect the most sophisticated attackers.
- Stopping data loss: Inspection of data in-motion and at-rest prevents potential theft by an active attacker.

For a deeper dive into best practices for protecting your organization and to download the full Zscaler ThreatLabz 2024 Phishing Report, visit http://www.zscaler.com/campaign/threatlabz-phishing-report.

**Methodology**
Zscaler ThreatLabz analyzed 2 billion blocked phishing transactions between January and December 2023, exploring various aspects including top phishing attacks, targeted countries, hosting countries for phishing content, distribution of company types based on server IP addresses, and the top referrers linked to these phishing attacks.

**About Zscaler**
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

**Media Contact**
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/a3ef271b-d70a-462e-92b9-848fb70e37e4