Zscaler ThreatLabz Uncovers Surge in AI-Driven Cyberattacks Targeting Critical Business Operations

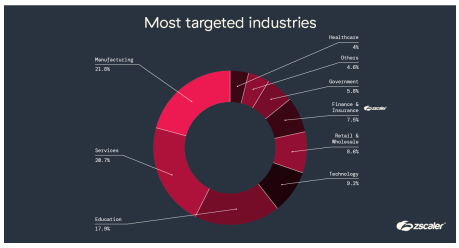
April 24, 2025

Zscaler's 2025 Phishing Report reveals cybercriminals are exploiting AI to launch precise attacks, underscoring the need for Zero Trust + AI powered defenses

Key Findings:

- **Global phishing is down 20%**, but attackers are striking deeper, not wider—targeting IT, HR, finance, and payroll teams with high-impact campaigns.
- **Telegram, Steam, and Facebook** are top platforms for phishing – used for both impersonation and malware delivery.
- **Tech support and job scams increase** with 159M+ hits in 2024, preying on users across social platforms.

Zscaler 2025 Phishing Report



Most Targeted Industries

SAN JOSE, Calif., April 24, 2025 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today published its Zscaler ThreatLabz 2025 Phishing Report, analyzing over two billion blocked phishing attempts between January and December 2024 captured by the Zscaler Zero Trust Exchange™, the world's largest cloud security platform. The annual report exposes how cybercriminals are using Generative AI to launch surgical, targeted attacks against high-impact business functions – and why a Zero Trust + AI defense strategy is mission critical. The report uncovers a shift from high-volume email blasts to targeted, AI-fueled attacks designed to evade defenses and exploit human behavior. It also offers actionable insight to help organizations defend against this evolving threat landscape.

"The phishing game has changed. Attackers are using GenAI to create near-flawless lures and even outsmart AI-based defenses," said Deepen Desai, CSO and Head of Security Research, Zscaler. "Cybercriminals are weaponizing AI to evade detection and manipulate victims, which means organizations must leverage equally advanced AI-powered defenses to outpace these emerging threats. Our research reinforces the importance of adopting a proactive, multi-layered approach—combining robust zero trust architecture with advanced AI-driven phishing prevention—to effectively combat the rapidly evolving threat landscape."

Emerging markets see a surge in phishing activity
While phishing dropped overall by 20% globally and by nearly 32% in the U.S., due in part to rising email authentication standards, attackers transitioned just as fast, launching more attacks on emerging markets like **Brazil, Hong Kong, and the Netherlands**, often where digital adoption outpaces security investment. Established targets like **India, Germany, and the UK** remain under sustained pressure, as threat actors adapt to local patterns and seasonal trends.

Community platforms fuel phishing growth
Phishing campaigns are increasingly abusing community-based platforms like **Facebook, Telegram, Steam, and Instagram** – not only spoofing their brands, but using them to distribute malware, mask C2 communications, gather target intel, and carry out social engineering attacks. Meanwhile, tech support scams, where attackers pose as IT support teams to exploit urgency and safety concerns of victims, remain widespread with **159,148,766 hits in 2024**.

Threat actors capitalize on AI: Phishing-as-a-Service and AI deception on the rise
Cybercriminals are using GenAI to scale attacks, generate fake websites, and craft deepfake voice, video, and text for social engineering. New scams mimic AI tools – such as resume generators and design platforms – tricking users into handing over credentials or payment data. Critical departments like payroll, finance, and HR are prime targets, along with executives – as they hold the keys to sensitive systems, information, and processes, and can more easily approve fraudulent payments.

Cybercriminals are also creating fake "AI assistant" or "AI agent" websites, falsely offering services such as resume generation, graphic design, workflow automation, and more. As AI tools become increasingly integrated into daily life, attackers are capitalizing on the ease of use and trust around AI to drive unsuspecting users to fraudulent sites.

Zscaler can help: Defending against AI threats with Zero Trust everywhere + AI
As cybercriminals continue to use GenAI to develop new tactics and deliver more sophisticated attacks, enterprises need to strengthen their defenses against every type of compromise.

The Zscaler Zero Trust Exchange protects users, applications, and data across all phases of the attack chain by:

- Minimizing the attack surface
- Preventing initial compromise
- Eliminating lateral movement
- Shutting down insider threats
- Stopping data loss

Zscaler AI-powered offerings add advanced protection by securing public AI use, shielding private AI models, and detecting AI-generated threats.

Download the Report
Get the full ThreatLabz 2025 Phishing Report to explore emerging trends and attack vectors. Learn why a Zero Trust + AI approach is critical to staying ahead of today's phishing threats. **Download today.**

Research Methodology
Zscaler ThreatLabz analyzed 2 billion blocked phishing transactions between January–December 2024, exploring various aspects including the 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. Additionally, ThreatLabz tracked and examined notable phishing trends and use cases observed throughout 2024.

About ThreatLabz
ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

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 SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Media Contacts
Nick Gonzalez
Sr. Manager, Media Relations
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/6b96dd38-9f87-4353-85b3-13a0086fc129