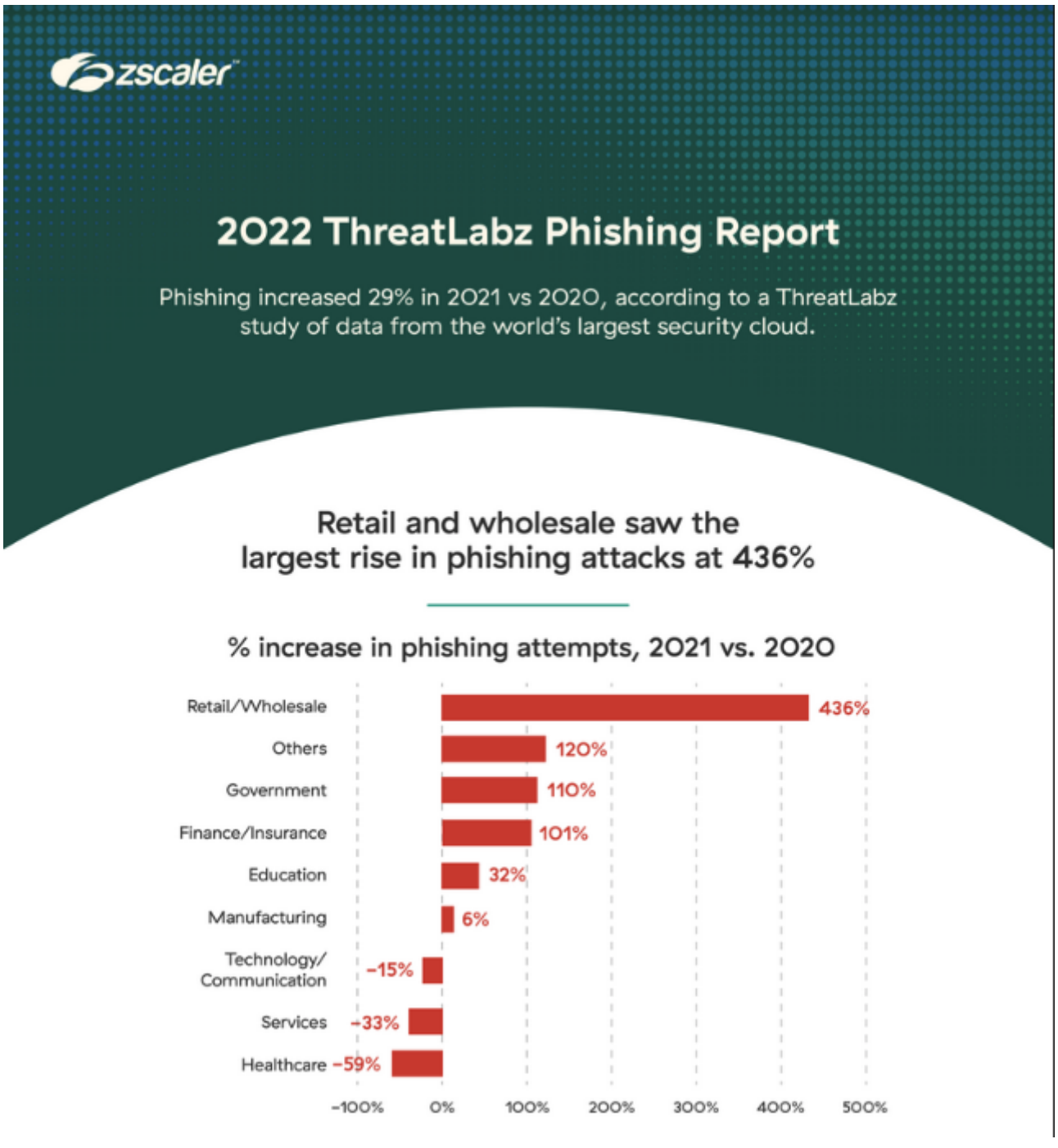
Download your free copy of the 2022 ThreatLabz Phishing Report, and check out our infographic.

For decades, phishing has been a complex and time-consuming challenge for every security team. As the findings of the ThreatLabz 2022 Phishing Report reveal, the challenge is getting harder: adversaries are getting craftier, and attackers are growing in numbers due to pre-built phishing kits available on the darknet. In this annual report, ThreatLabz offers deep insights on the current phishing threat landscape from a full year's worth of phishing data from the world's largest security cloud. Avoiding the latest breed of phishing attacks requires heightened awareness from users, additional context, and a zero trust approach.

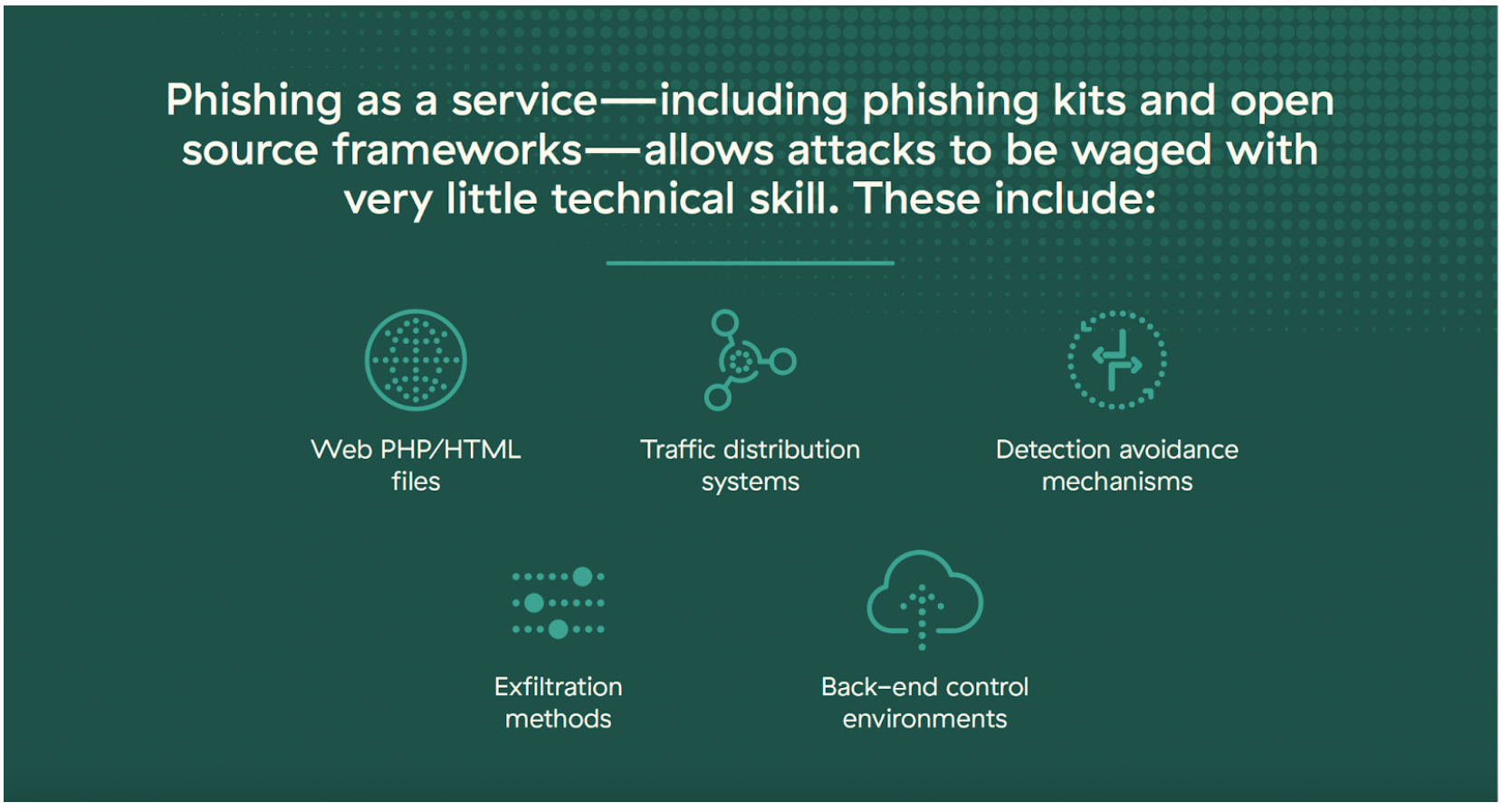


Report Highlights

From imitating popular brands like Microsoft to buying advertisements on Google and other search platforms, threat actors use a range of tactics and techniques to trick users into giving up sensitive information. Analyzing data from more than 200 billion daily transactions last year, the 2022 report found that:

Phishing attacks rose 29% in 2021 compared to 2020, driven by multiple trends:

- COVID-19 and work-from-home: Consumers engaged in more activities online, giving attackers new ways to take advantage.
- Better threat protection: Organizations have been improving their threat prevention capabilities, leading attackers to use more sophisticated methods. Phishing provides adversaries with legitimate login credentials, allowing them to subvert security controls and compromise systems.
- Phishing-as-a-service: Phishing kits package up pre-built tools to make phishing attacks easier to wage (even by adversaries who lack strong technical skills), and harder to spot for security teams.



More than 96% of attacks in our study lacked a referring domain, indicating that the victim clicked a direct link to the phishing site through their email, SMS, or another client. Email continues to be the top phishing vector, but other vectors such as SMS are growing: consumers trust text messages more than emails, and a successful SMS phishing ("SMiShing") attack can give attackers the smartphone access that they need to bypass two-factor authentication. The top 20 referring domains included search platforms, corporate forums and marketplaces, sharing sites, e-commerce tools, and others.

Retail and wholesale saw a massive 436% leap in phishing attacks in 2021 as attackers took advantage of COVID-boosted online shopping trends. Retail and wholesale moved from the fifth-most phished industry category all the way to first, ahead of last year's most phished industry, manufacturing.

The United States is (once again) the most targeted country in our study with more than 60% of phishing attempts. However, phishing only rose 7% in the United States in 2021, whereas the increase was much higher elsewhere. ThreatLabz breaks down the full list of the 10 most targeted countries with details on which countries saw the sharpest increases in phishing attacks during 2021.

Additionally, in this year's report, ThreatLabz analyzes popular techniques used by phishing threat actors and explores some of the key drivers intensifying enterprise risk, including:

- Top targeted geographies and industry verticals
- Personalization and highly targeted attacks
- Zero-day vulnerabilities and rapid exploits
- Phishing-as-a-service and phishing kits
- Safe domains and trusted platforms

Improve Your Phishing Defenses

Industry statistics reveal that the average organization receives dozens of phishing emails daily, with financial losses snowballing as losses incurred from malware and ransomware attacks drive up the average costs of landed phishing attacks year over year. Facing all the threats outlined in this report is a big job, and while you can not completely eliminate the risk of phishing threats, you can learn from observed trends and incidents to better manage risk.

The basics for mitigating the risk of phishing attacks:

1. Understand the risks to better inform policy and technology decisions
2. Leverage automated tools and actionable intel to reduce phishing incidents
3. Implement zero trust architectures to limit the blast radius of successful attacks
4. Deliver timely training to build security awareness and promote user reporting
5. Simulate phishing attacks to identify gaps in your program

How the Zscaler Zero Trust Exchange Can Mitigate Phishing Attacks

User compromise is one of the most difficult security challenges to defend against. Your organization must implement phishing prevention controls as part of a broader zero trust strategy that enables you to detect active breaches and minimize damages caused by successful breaches. The Zscaler Zero Trust Exchange is built on a holistic zero trust architecture to minimize the attack surface, prevent compromise, eliminate lateral movement, and stop data loss. Zscaler helps stop phishing in the following ways:

- Prevents compromise: Full SSL inspection at scale, browser isolation, and policy-driven access control to prevent access to suspicious websites.
- Eliminates lateral movement: Connect users directly to apps, not the network, to limit the blast radius of a potential incident.
- Shuts down compromised users and insider threats: If an attacker gains access to your identity system, we can prevent private app exploit attempts with in-line inspection and detect the most sophisticated attackers with integrated deception.
- Stops data loss: Inspect data-in-motion and data-at-rest to prevent potential data theft from an active attacker.

Related Zscaler products:

Zscaler Internet Access helps identify and stop malicious activity by routing and inspecting all internet traffic through the Zero Trust Exchange. Zscaler blocks:

- URLs and IPs observed in Zscaler cloud, and from natively integrated open source and commercial threat intel sources. This includes policy-defined high-risk URL categories commonly used for phishing such as newly observed and newly activated domains.
- IPS signatures developed from ThreatLabz analysis of phishing kits and pages.
- Novel phishing sites identified by content scans powered by AI/ML detection.

Advanced Threat Protection blocks all known command-and-control domains.

Advanced Cloud Firewall extends command-and-control protection to all ports and protocols, including emerging C&C destinations. Cloud Browser Isolation creates a safe gap between users and malicious web categories, rendering content as a stream of picture-perfect images to eliminate the leakage of data and the delivery of active threats.

Advanced Cloud Sandbox prevents unknown malware delivered in second stage payloads.

Zscaler Private Access safeguards applications by limiting lateral movement with least privileged access user-to-app segmentation and full in-line inspection of private app traffic.

Zscaler Deception detects and contains attackers attempting to move laterally or escalate privileges by luring them with decoy servers, applications, directories, and user accounts.

Learn more

Download the 2022 Phishing Report by ThreatLabz to learn more about the latest trends in phishing attacks and to discover:

- Overview of 21 common phishing attack types, 11 scam categories, and threat analysis of the TTPs used in popular and emerging scams

- How the phishing threat landscape has shifted towards specialization and automation, making it easier for threat actors to launch more potent campaigns than ever before
- Best practices for identifying attacks and improving your phishing defenses
- How zero trust can fortify your organization against phishing attacks
- 2023 phishing trend predictions

Get your copy here.

About us

Zscaler ThreatLabz is a global threat research team with a mission to protect customers from advanced cyberthreats. Made up of more than 100 security experts with decades of experience in tracking threat actors, malware reverse engineering, behavior analytics, and data science, the team operates 24/7 to identify and prevent emerging threats using insights from 300 trillion daily signals from the Zscaler Zero Trust Exchange.

Since its inception, ThreatLabz has been tracking the evolution of emerging threat vectors, campaigns, and groups, contributing critical findings and insights on zero-day vulnerabilities, ——including active IOCs and TTPs for threat actors, malware, and ransomware families, phishing campaigns, and more.

ThreatLabz supports industry information sharing and plays an integral role in the development of world-class security solutions at Zscaler. See the latest ThreatLabz threat research on the Zscaler blog.

- Security Research
- Insights and Research
-

Authors

Rohit Hegde

Jim Wang

Recommended for You

The Latest Sandworm Botnet Attack Shows Why Firewalls Can't Do Zero Trust

The Top 5 Benefits of a Cloud-Native Application Protection Platform (CNAPP)

FFDroider Stealer Targeting Social Media Platform Users

Analysis of Spring Cloud Framework Vulnerabilities