Kaseya®

WHITEPAPER

The top 25 most-phished brands

The top 25 most-phished brands

The numbers are in. The top 25 most-phished brands of 2025 represent the organizations attackers most frequently impersonated in email-based attacks detected by INKY. Using a combination of AI and GenAI capabilities, INKY renders every email and applies computer vision algorithms to "see" each email as a human recipient would see it. This helps identify brand impersonation attempts through image segmentation, semantic image classification and logo recognition.

These brands rose to the top out of 281 unique brands impersonated during the second half of 2025. To put the scale into perspective, INKY processed more than 4.5 billion emails over the course of the year. Within that volume, 5,283,200 phishing emails were associated with the top 25 brands alone.

All of these attacks were successfully detected and blocked before reaching end users, preventing the downstream impacts such as credential theft, fraud and ransomware that brand impersonation phishing is designed to enable.

In total, 6,688,601 brand impersonation emails were detected in the second half of 2025 alone through INKY's anti-phishing capabilities. This report ranks these brand impersonations by frequency and details how they were used in attempts to breach targeted networks.

Top 25 brands detected by INKY

Brand name	Email count	Sector	% of brand impersonations
Microsoft	1,970,310	Technology	29.46%
Docusign	1,041,822	Technology	15.57%
Amazon	265,291	Retail	3.96%
Intuit	240,286	Finance	3.59%
LinkedIn	184,330	Technology	2.75%
Costco	144,057	Retail	2.15%
Intermedia	113,207	Telecommunications	1.69%
ADP	104,630	Technology	1.56%
Apple	100,997	Technology	1.51%
Morgan Stanley	98,545	Finance	1.47%
Ring Central	89,831	Telecommunications	1.34%
Chase	88,441	Finance	1.32%
PayPal	87,900	Finance	1.31%
Google	87,668	Technology	1.31%
Adobe	79,238	Technology	1.18%
Zoom	74,944	Telecommunications	1.12%
State Farm	68,662	Finance	1.02%
Facebook	64,139	Technology	0.95%
CVS	58,432	Retail	0.87%
U.S. Postal Service	58,101	Logistics	0.86%
Lexis Nexis	57,632	Technology	0.86%
Verizon	55,011	Telecommunications	0.82%
Bank of America	54,212	Finance	0.81%
Bamboo HR	51,761	Technology	0.77%
UPS	43,753	Logistics	0.65%
Total	**5,283,200**		

Overview

Microsoft was, unsurprisingly, the most-phished brand by a wide margin, accounting for nearly 30% of all brand impersonation emails in 2025 (Top 25 brands detected by INKY). Microsoft has consistently been the most-impersonated brand year after year, driven by the fact that its broad ecosystem touches nearly every business. From an attacker's perspective, it is a safe assumption that most recipients have some form of Microsoft account.

With other brands, an email from a brand the recipient has no relationship with can be an immediate red flag, causing the message to more likely be recognized as a phishing attack. For example, someone who doesn't have a Bank of America account receiving an email about updating their banking information, will most likely question its legitimacy. A closer look at the top 10 brands shows Microsoft firmly in the lead, followed by other widely recognized household names. (Figure 1).

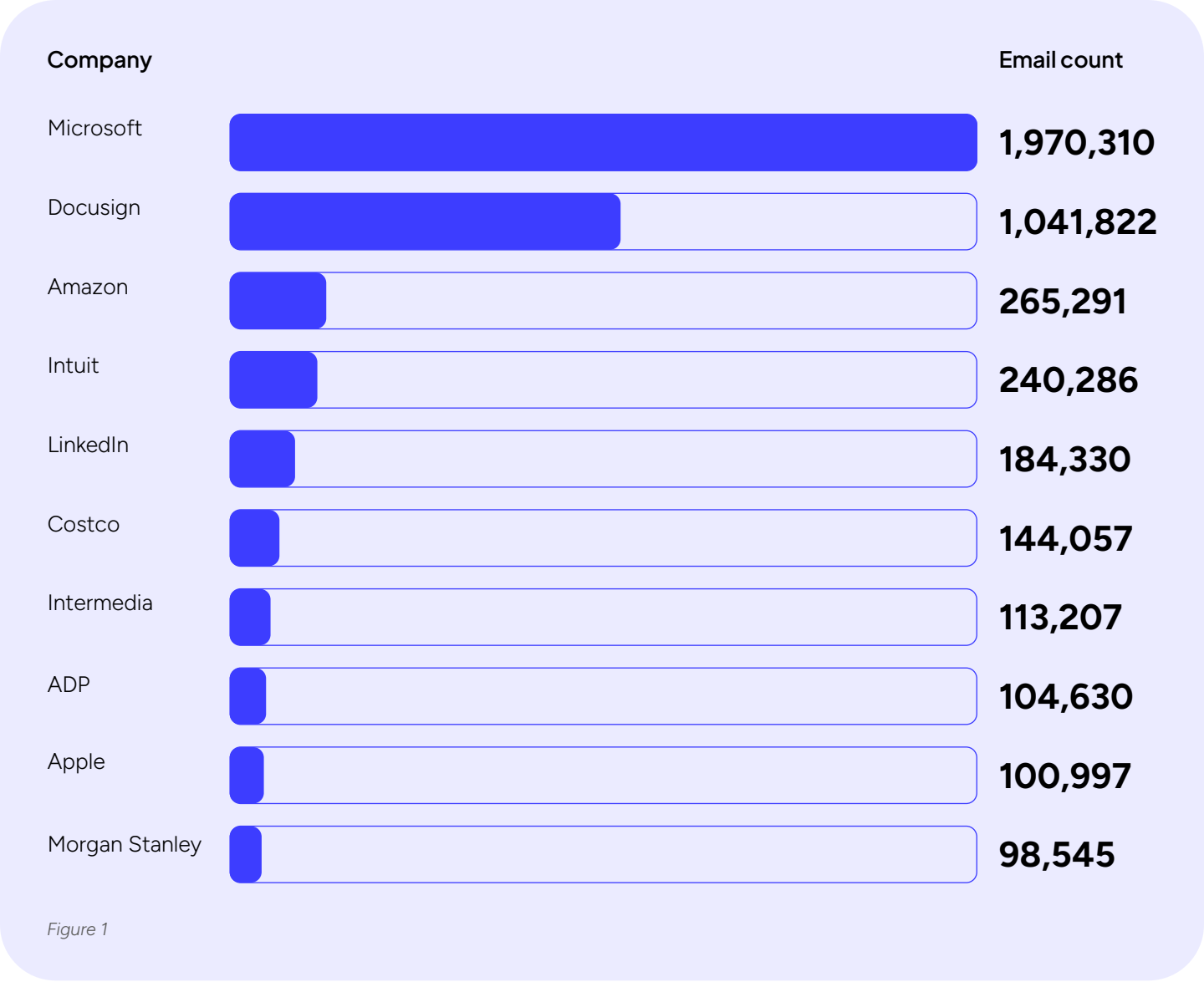

Figure 1

Top industries targeted through brand impersonation

Looking at brand impersonation by sector reveals how attackers prioritize opportunity over novelty. Certain industries naturally lend themselves to phishing because their communications are frequent, time-sensitive and expected by recipients. Sector-level analysis highlights where attackers expect urgency, financial access or account authority to override skepticism. This helps clarify why certain industries consistently dominate impersonation trends year after year.

A look at the domain-impersonation data by sector reveals Finance well in the lead, followed by Technology, Retail, Telecommunications and Logistics (Figure 2).

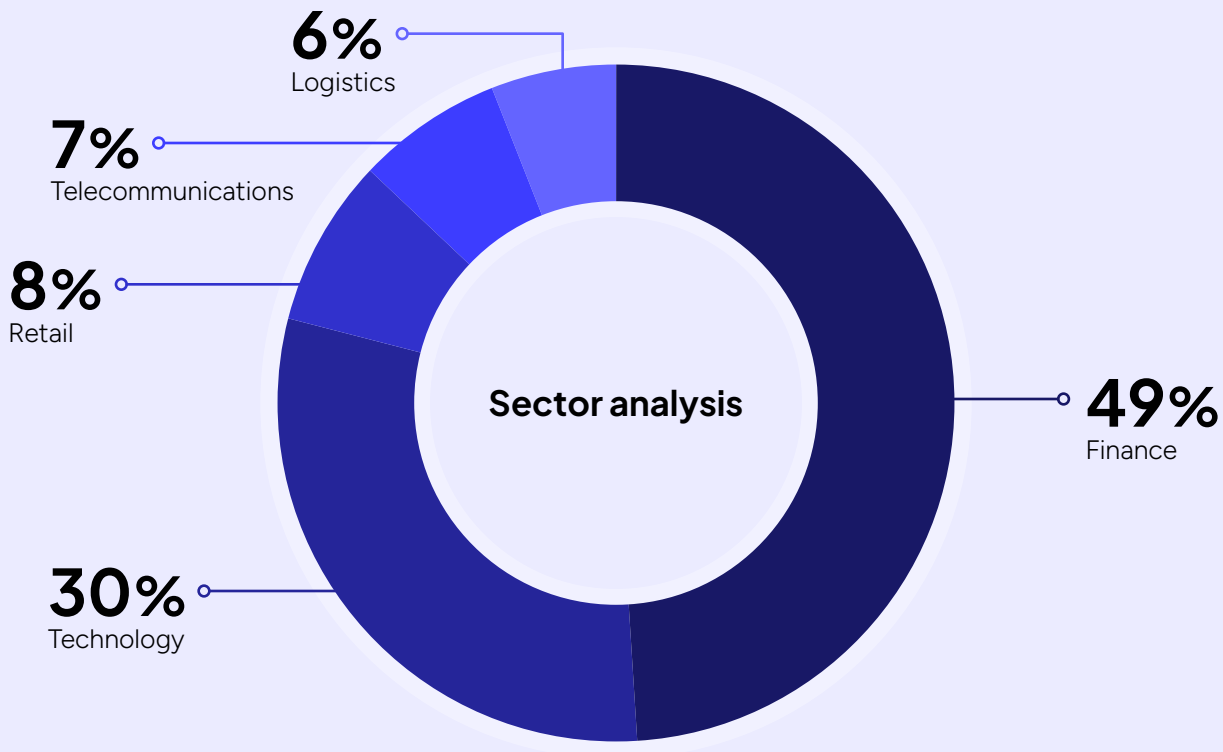

Figure 2

Finance

Multiple financial organizations appeared in the top 25, including Intuit, Morgan Stanley, Chase Bank, PayPal, State Farm and Bank of America (Figure 3). And, of course, the "Willie Sutton rule" applies here as well: attackers impersonate banks because that is where the money is.

Intuit	Morgan Stanley	Chase
240,286	98,545	88,441

Paypal	State Farm	Bank of America
87,900	68,662	54,212

Figure 3

PayPal was the fourth most-impersonated finance brand in 2025. One increasingly common technique involves attackers abusing legitimate online services to send emails that appear to originate directly from PayPal while containing misleading content. This email (Figure 4) is a good example of INKY's Computer Vision capabilities. The email was in fact an image and not actually text.

These messages are difficult to distinguish from legitimate notifications and often bypass legacy email security systems. PayPal alerts related to investigations, account limitations or case reviews to create urgency and manipulate victims into clicking links, calling phone numbers or providing sensitive information. (Figure 5).

GS

George Smith
Your confirmation at your convenience is requested
To: -----

Yesterday at 9:25 AM

PayPal

Transaction Alert

Dear George,

We noticed an unauthorized transaction from your digital wallet.

IF THIS TRANSACTION IS NOT MADE BY YOU THEN KINDLY CONTACT US FOR CANCELLATION OF THIS ORDER OTHERWISE YOUR $568.69 USD USD WILL BE CHARGED TODAY.

FOR CANCELLATION: **+1 (806) 250 7123**

Description	Amount (USD)	Qty	Total
Digital Asset Purchase	$568.69 USD	0.004925	$568.69 USD

Tax / Fees	$0
Total Charged	**$568.69 USD**
Amount Due (if not canceled)	**$568.69 USD**

Figure 4

Seller name	PayPal open a case against your transaction. If you did not authorize this charge, Please call PayPal at **+1(833) 307-4409** to request a refund We are waiting for your response. If we do not hear from you within 24 hours, we will release this payment, and a refund will no longer be possible.

Figure 5

Next on the list of impersonated financial brands is Intuit, a fully cloud native, with its flagship SaaS product QuickBooks Online serving as one of the world's most-widely used accounting platforms. QuickBooks dominates the small business accounting market with more than 7 million global active users and 23,682 verified companies relying on it for daily financial operations. A perfect hole to phish for money. Here's a notice from a generic "Accounts Payable Executive," authorizing a direct deposit with more details in the attached file. (Figure 6). The attached file will drive you to a fraudulent login page designed to harvest your account credentials.

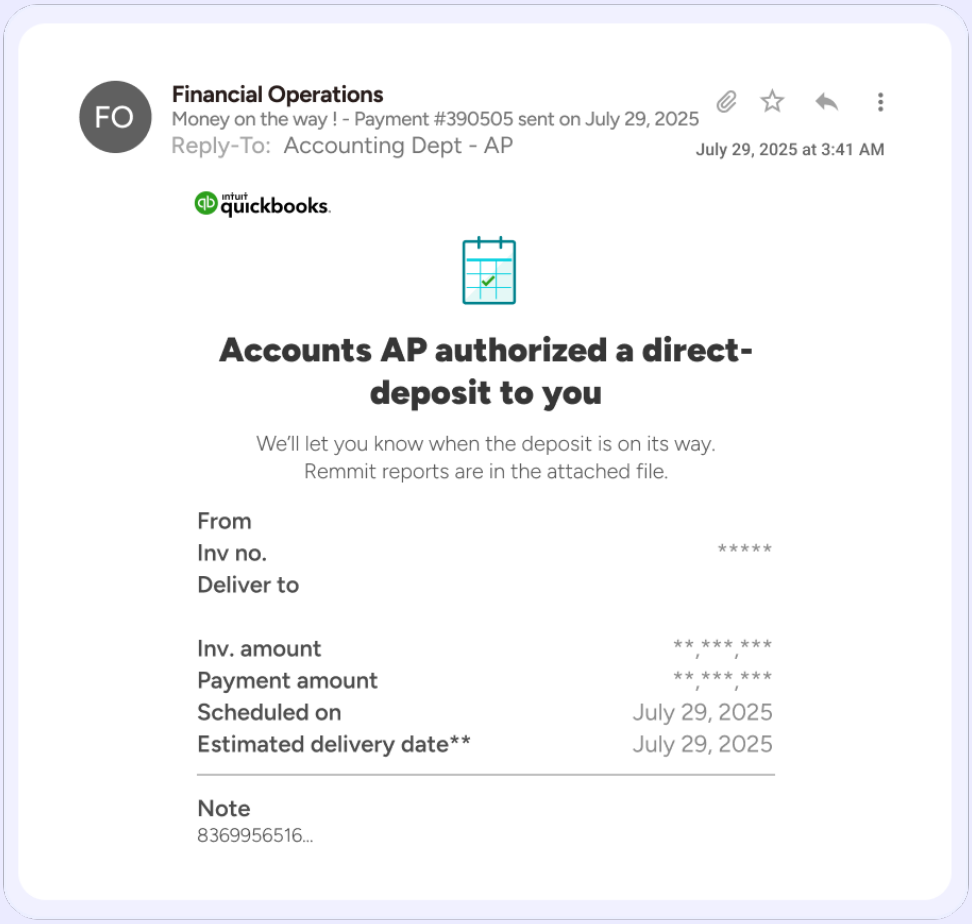

Figure 6

Technology

Microsoft was by far the most-impersonated brand in 2025. Microsoft credentials are highly prized in business email compromise (BEC) schemes. Once attackers gain access to an account, they quietly exfiltrate email data to study buyer-supplier relationships. As they learn about an organization's payment patterns and supply chain, they wait for the right moment to divert payments. Armed with stolen messages and contextual details, they craft lookalike domains or spoof trusted senders, deceiving employees into sending funds to fraudulent accounts. Considering how widespread Microsoft impersonation has become, it's clear that this tactic has become a highly profitable criminal enterprise.

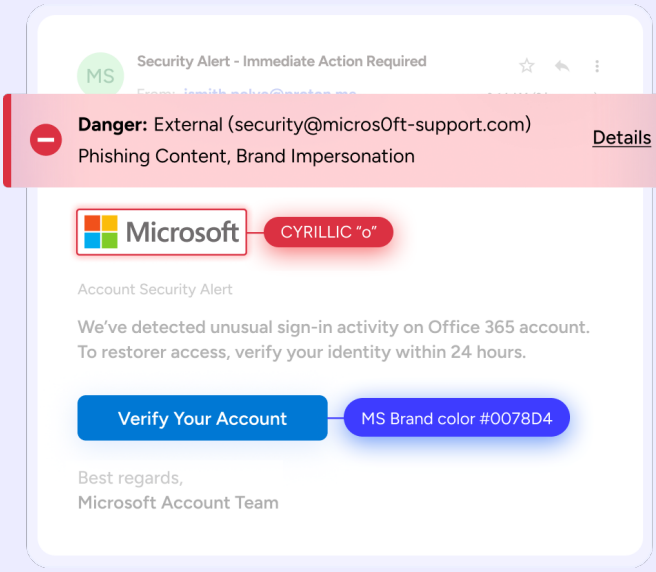

Figure 7

One common method used in these attacks is credential harvesting. Victims are prompted to "log in" to their Microsoft account, where the landing page convincingly mimics Microsoft branding but is controlled by the attacker (Figure 7). Screenshots throughout this report obscure company-specific and personal details for privacy reasons.

Another growing technique involves malicious QR codes. These are increasingly being used to steal employee credentials as QR code adoption surges. Attackers send phishing emails that impersonate Microsoft, often appearing to come from within the organization, and urge employees to address urgent account issues such as 2FA setup, password verification or account lockout prevention. These messages rely on image-based phishing tactics, create a strong sense of urgency and warn of consequences for inaction (Figure 8). Employees are ultimately prompted to scan a fraudulent QR code in the email, leading them to fake login page designed to steal your account credentials.

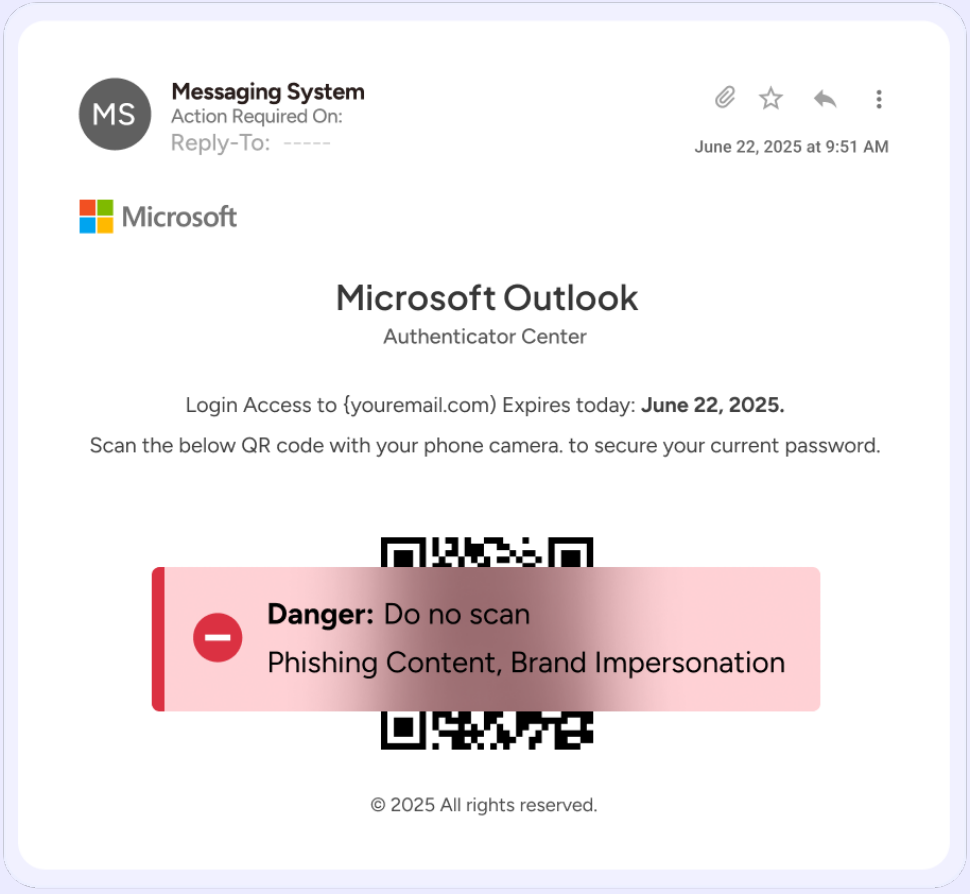

Figure 8

The combination of recognizable workflows, trusted brands, and routine business communications places many technology brands among the most impersonated targets in phishing attacks. Other technology brands appearing in the top 25 include DocuSign, LinkedIn, ADP, Apple, Google, Adobe, Facebook, Lexis Nexis and Bamboo HR (Figure 9).

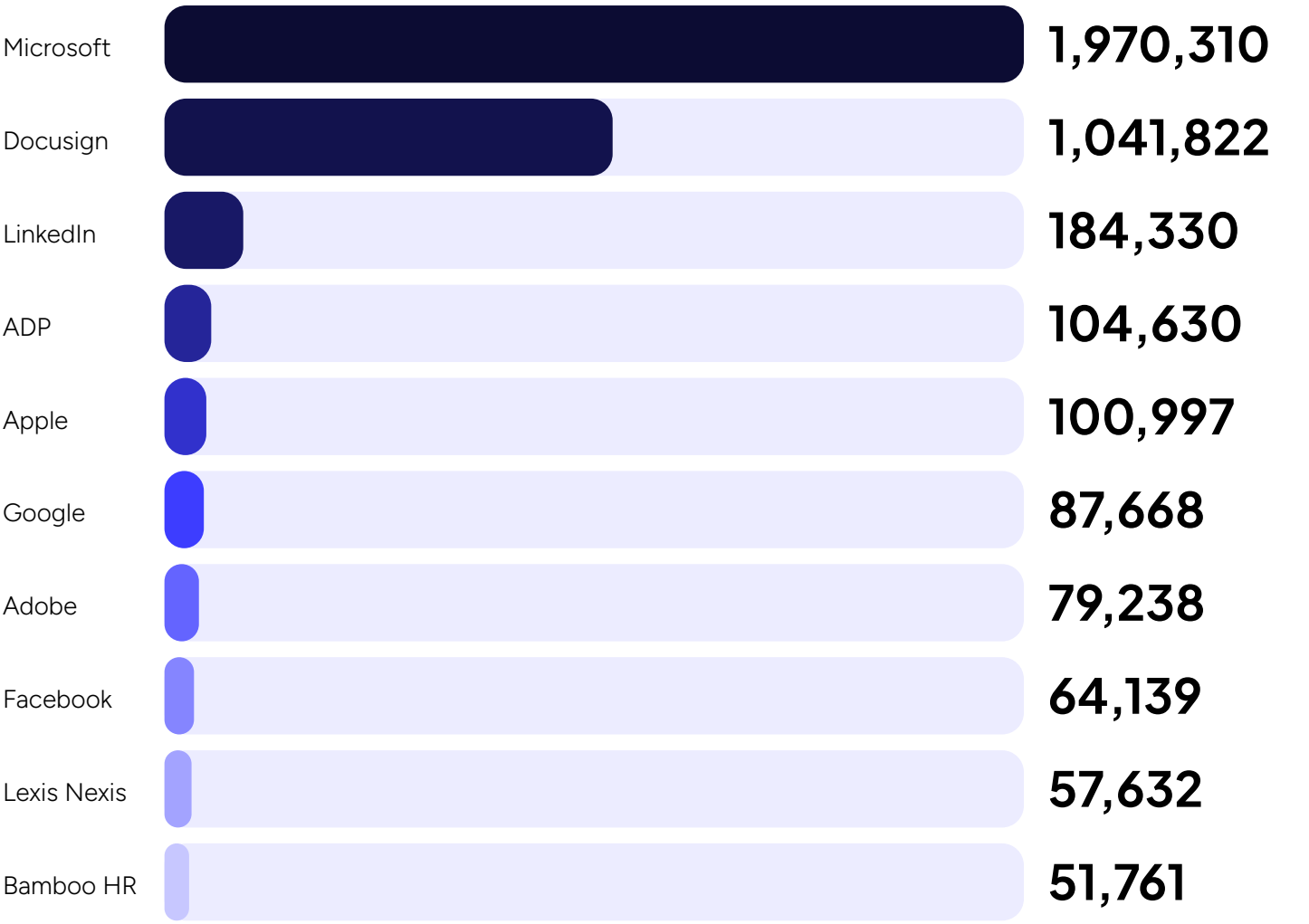

Figure 9

DocuSign ranked next within the technology category. Its rapid growth during the pandemic — and continued adoption since — made it a familiar and trusted part of everyday business workflows. As DocuSign usage expanded, attackers increasingly exploited its recognizable branding, resulting in a rise in phishing attacks that closely mimic its visual elements and transaction notifications (Figure 10).

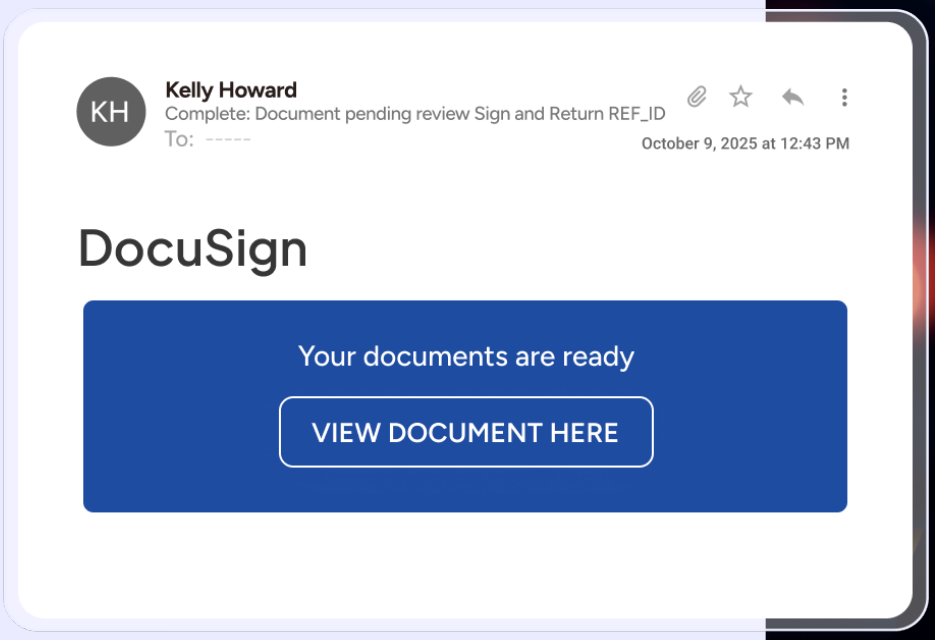

Figure 10

Retail

Continued growth in online shopping placed retail third among the most-impersonated sectors in 2025. Amazon, Costco and CVS ranked among the top 25 most-impersonated brands, as attackers increasingly launched high-volume phishing campaigns targeting retail customers (Figure 11).

Amazon's vast scale in 2025 makes it an especially attractive target for impersonation, processing nearly **12 million orders per day**, with roughly 208 million in the U.S. alone.

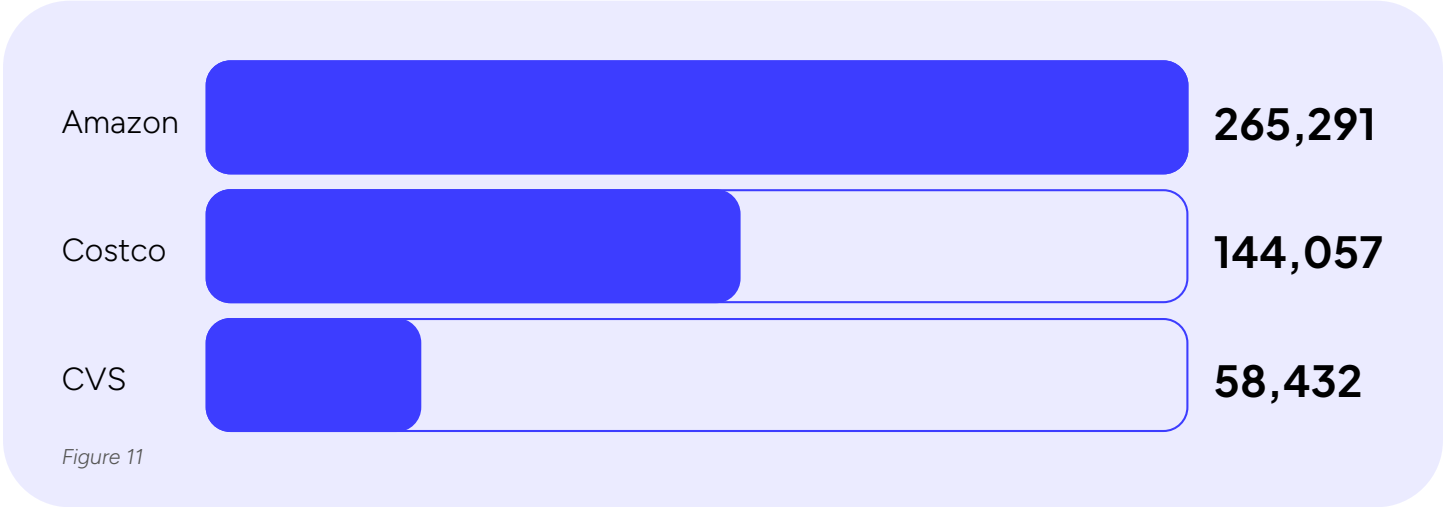

Figure 11

This convincing spoof of a Prime membership renewal email looks almost identical to real Amazon emails but contains malicious links leading to a fake login page (Figure 12).

Another growing trend is phishing attacks that omit attachments and links altogether. This has been used in Amazon shipment notification emails where only a phone number is provided, driving victims into voice-based social engineering schemes in which attackers attempt to obtain login credentials and credit card details over the phone.

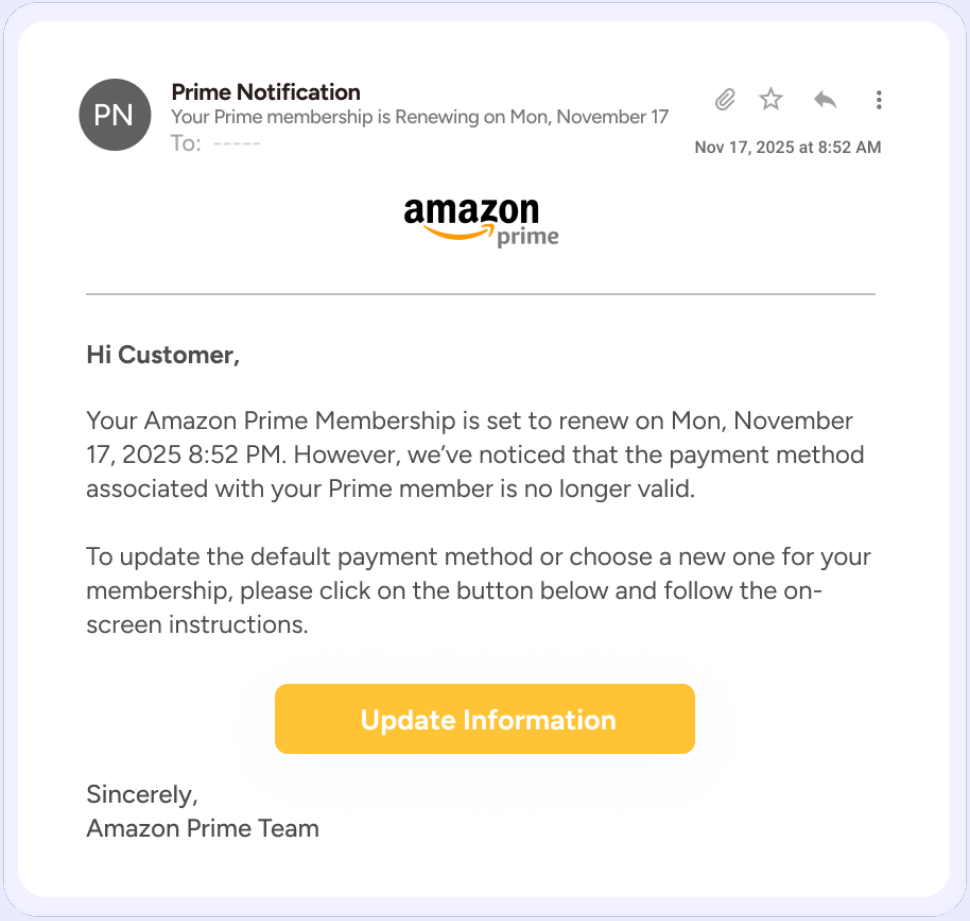

Figure 12

Telecommunications

Telecommunications ranked fourth among impersonated sectors in 2025. Brands providing wireless services, videoconferencing and VoIP platforms are deeply embedded in daily business operations and remote collaboration. Increased reliance on these services has made them attractive targets for phishing campaigns. Intermedia was the most-impersonated telecommunications brand, followed by RingCentral, Zoom, Verizon and AT&T (Figure 13).

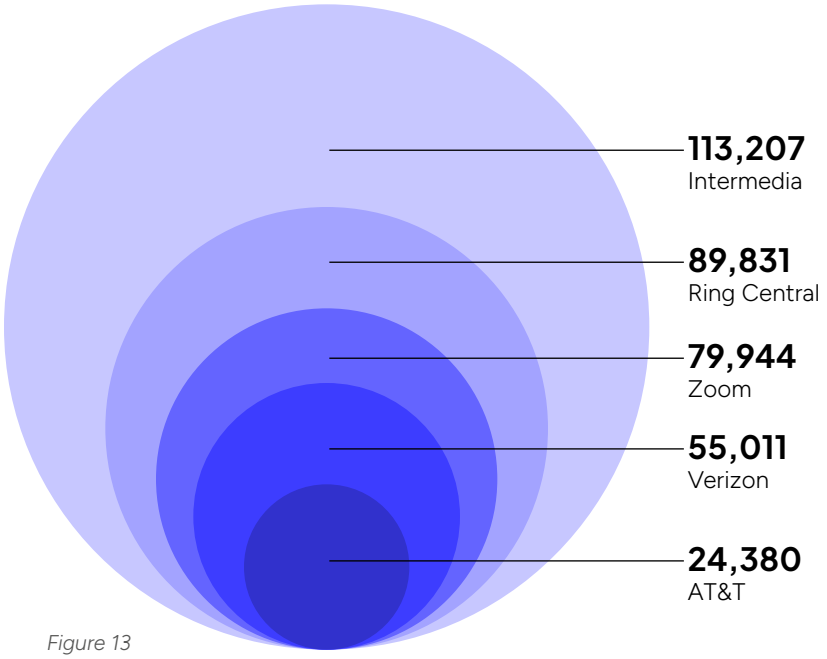

Figure 13

Attackers exploit the frequency of virtual meetings to create a sense of urgency and normalcy. A common attack method is harvesting credentials through a Zoom meeting invite (Figure 14). When recipients clicked the link, they were taken to a convincing but fraudulent, Zoom login page. Attackers have also used similar tactics to harvest Microsoft Office365 and Outlook credentials, beginning with a spoofed Zoom meeting invitation.

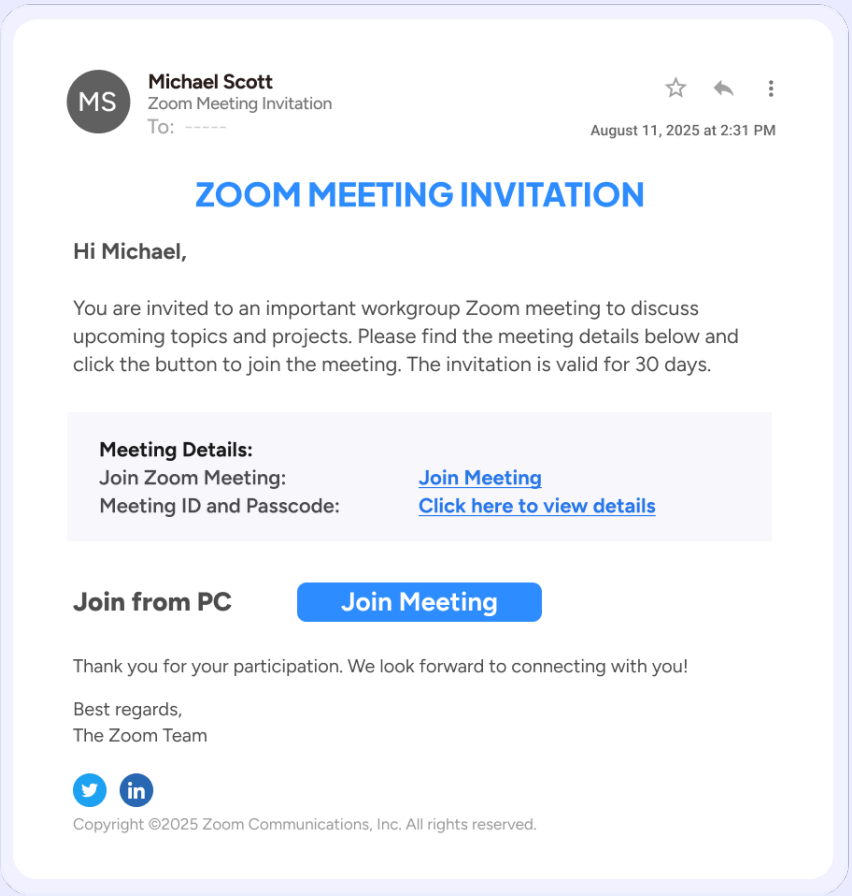

Figure 14

Logistics

Logistics companies experienced a sustained rise in impersonation attempts as global shipping volumes continued to grow. With millions of packages delivered daily to homes and offices, attackers rely on shipping notifications to create urgency and legitimacy. The U.S. Postal Service and UPS were the most impersonated logistics brands in 2025 (Figure 15).

USPS	UPS
58,101	43,753

Figure 15

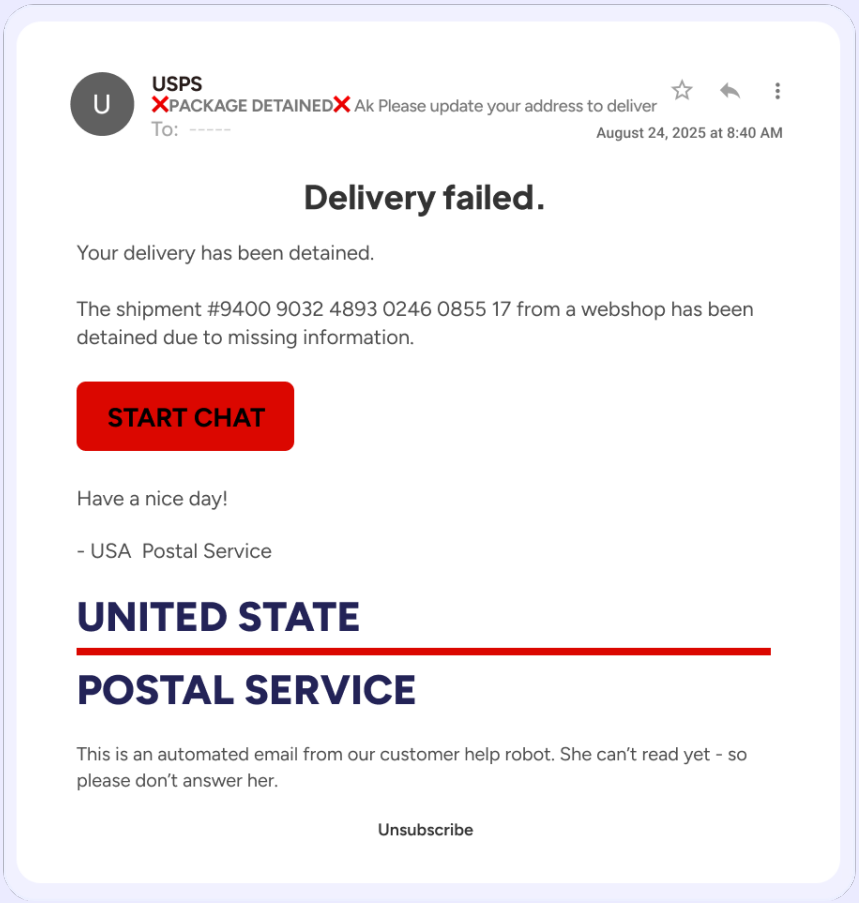

Figure 16

The U.S. Postal Service sits at the top of logistics impersonated brands in 2025. As with many of these attempts, this one has a note of urgency about it: take some action quickly (start a chat) to avoid an issue with a delivery (having the package returned or "detained"). (Figure 16)

Why today's phishing is harder to detect

Phishing attacks remain cybercrime's most common — and most damaging — entry point. According to the FBI's Internet Crime Report, phishing activity surged dramatically in 2024, with reported losses climbing **274% from $18.7 billion in 2023 to $70 billion in 2024**[1]. This explosive growth reflects a shift in attacker strategy: rather than relying on malware-heavy campaigns, modern phishing increasingly exploits trusted brands, familiar workflows and human decision-making to bypass technical defenses.

Recent research shows that **83% of phishing emails now contain AI-generated or AI-assisted content**[2]. Generative AI enables attackers to rapidly produce realistic branding, natural language and personalized lures at scale. Common tactics include prize scams, QR-code-based credential theft and messages designed to resemble routine business communications, making them difficult for both users and traditional security tools to identify.

Why INKY catches what other anti-phishing solutions miss

INKY's AI capabilities include performing computer vision analysis in a secure browser environment. Logos, branding elements and layout patterns are extracted and compared against known brand assets and the actual sending domain.

This approach enables INKY to detect brand forgery and lookalike attacks even when no malicious payload is present and the sender infrastructure appears legitimate. By focusing on visual context, semantic intent and brand authenticity, INKY identifies sophisticated impersonation attacks that routinely bypass legacy email security solutions.

Stop email threats before they reach your users

Kaseya's GenAI-powered email security solution, INKY, continuously scans emails to detect and prevent phishing attempts. It neutralizes harmful messages before they can compromise user accounts or infiltrate your organization.

Learn more

Sources:
1 https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report
2 https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report

Kaseya®

Kaseya is the leading global provider of AI-powered IT management and cybersecurity software. Kaseya delivers a unified technology platform to manage infrastructure, secure endpoints, back up critical data, and streamline operations for more than 40,000 MSP and SMB customers around the globe. To learn more, visit www.kaseya.com.

kaseya.com