Phishers' Favorites

2023 Year-in-Review

www.vadesecure.com

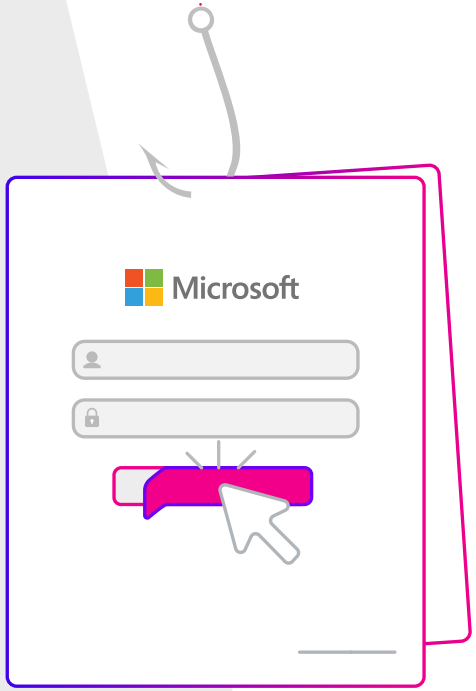
CONTENTS

Phishers' Favorites Year-in-Review

THE TOP 20 MOST IMPERSONATED BRANDS IN PHISHING ATTACKS

Phishers' Favorites Year-in-Review is Vade's annual report highlighting the top 20 most impersonated brands in phishing attacks and explores key phishing trends from the year.

Each quarter, Vade's filter engine detects and analyzes millions of phishing emails and hundreds of thousands of phishing webpages. The top brands in phishing are determined by analyzing unique, branded phishing websites. Cybercriminals often send dozens, and sometimes hundreds or thousands of phishing emails containing the same unique phishing link, while a single domain can host thousands of phishing URLs.



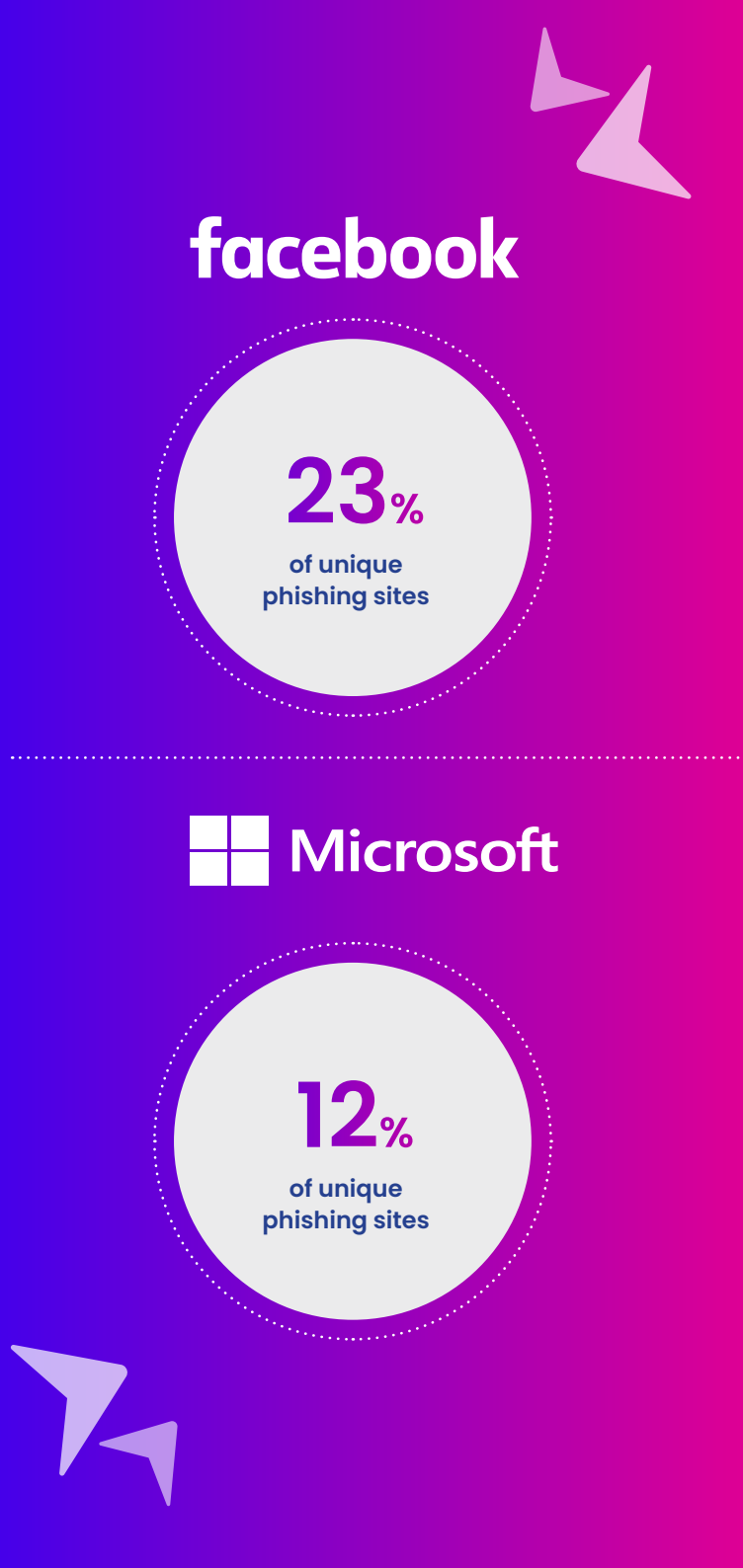
THE TOP 20 MOST IMPERSONATED BRANDS IN PHISHING ATTACKS

In 2023, brands featured in the Phishers' Favorites report accounted for more than 197,000 unique phishing websites. While the uniqueness decreased by 28% year-over-year (YoY), the figure accompanies a period that saw the highest annual total of phishing URLs sent globally on record (more than 1.76 billion).

For the third straight year, Facebook was the most impersonated brand, nearly doubling the unique phishing URLs of the runner up on the list, Microsoft. Facebook accounted for more than 44,000 branded phishing websites—representing 23% of phishing URLs from this year's list. The brand also set an organizational record, eclipsing any other year to date since Vade began tracking these statistics. While impersonation attempts increased 74% YoY, most of this increase happened during H2. In Q3, Facebook saw a 169% increase in unique phishing URLs QoQ. In Q4, volumes held steady, falling slightly by 5%.

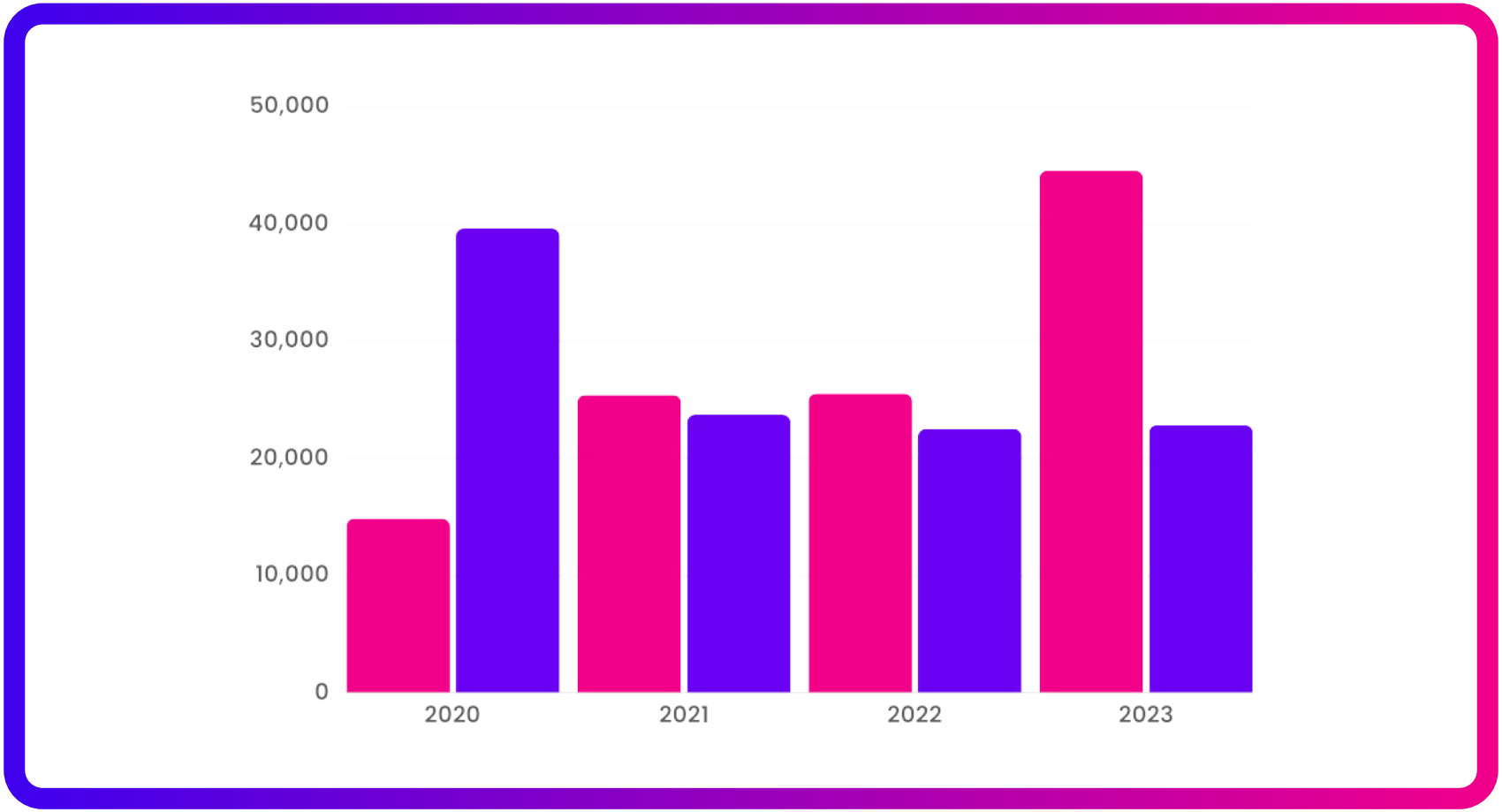
This year's figures only further strengthened Facebook's reign as the most impersonated brand, continuing the trend for the third straight year. The brand's popularity among hackers illustrates the prominence of social media phishing as a vector.

While Facebook's phishing stats stand out, Microsoft also finished 2023 as a perennial phishers' favorite. Since 2022, the cloud leader saw a slight increase (1% YoY) in unique phishing URLs to finish at more than 22,000. Microsoft accounted for nearly double the total of the next place finisher.



THE TOP 20 MOST IMPERSONATED BRANDS IN PHISHING ATTACKS

Since 2020, the title of the most impersonated brand has flip-flopped between Facebook and Microsoft—a trend that shows no signs of changing in the year to come.



Facebook and Microsoft annual phishing URLs, 2020 - 2023

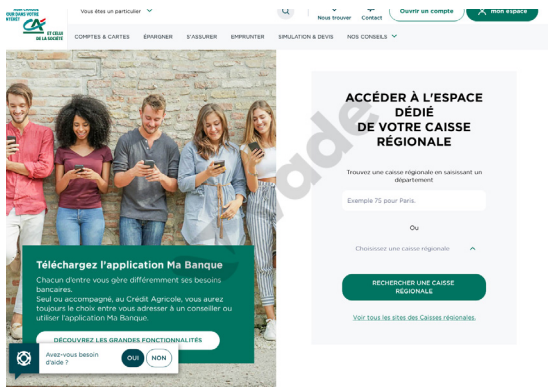
THE TOP 20 MOST IMPERSONATED BRANDS IN PHISHING ATTACKS

While Facebook and Microsoft made headlines, **Crédit Agricole finished as the third most spoofed brand**, after ending 2022 in the seventh spot. The company led all other financial services brands with more than double the number of unique phishing URLs than the next place finisher. This represents the second time since 2021 that the brand has finished as the third most spoofed brand.

Rounding out the remainder of the top ten were Orange, SoftBank, Amazon, PayPal, Apple, Bank of America, and Instagram. Orange and Amazon both ended the year leading their respective industries (Internet/telco and e-commerce/logistics). After ending 2021 and 2022 in sixth place, Orange for the first time broke into the top 5.

Notably, SoftBank, Amazon, Bank of America, and Instagram all finished outside the top 10 in 2022. Among these brands, **SoftBank made the biggest jump from 2022 to 2023**, moving up 76 spots to finish in the top 5.

Google, which finished 2022 as the third most spoofed brand, ended the year in 11th place.
In other notable developments, SFR and American Express also entered the top 20, while MTB, au, WellsFargo, Rakuten, Credit Saison, Adobe, and Santander dropped out. Meanwhile, La Banque Postale, WhatsApp, DHL, Comcast, OVH, Société Générale, and Netflix all featured among the top 20 for at least the second consecutive year.



Crédit Agricole impersonation

Phishers' Favorites 2023

20 MOST IMPERSONATED BRANDS

Number	Movement	Brand	Category	Unique Phishing URLs
1	0	Facebook	Social Media	44548
2	0	Microsoft	Cloud	22851
3	↑ 4	Crédit Agricole	Financial Services	11668
4	↑ 2	Orange	Internet/Telco	8719
5	↑ 76	SoftBank	Financial Services	5511
6	↑ 7	Amazon	E-Commerce/Logistics	4522
7	↓ -3	PayPal	Financial Services	4518
8	↑ 4	Apple	E-Commerce/Logistics	4472
9	↑ 14	Bank of America	Financial Services	4080
10	↑ 6	Instagram	Social Media	3763
11	↓ -8	Google	Cloud	2959
12	↓ -3	La Banque Postale	Financial Services	2828
13	↓ -5	WhatsApp	Social Media	2735
14	↑ 7	DHL	E-Commerce/Logistics	2694
15	↑ 11	SFR	Internet/Telco	2501
16	↑ 1	Comcast	Internet/Telco	2435
17	↑ 5	OVH	Internet/Telco	2283
18	↑ 7	Société Générale	Financial Services	2261
19	↓ -8	Netflix	Cloud	2239
20	↑ 12	American Express	Financial Services	1718
				139305

Added:
SoftBank, SFR, American Express

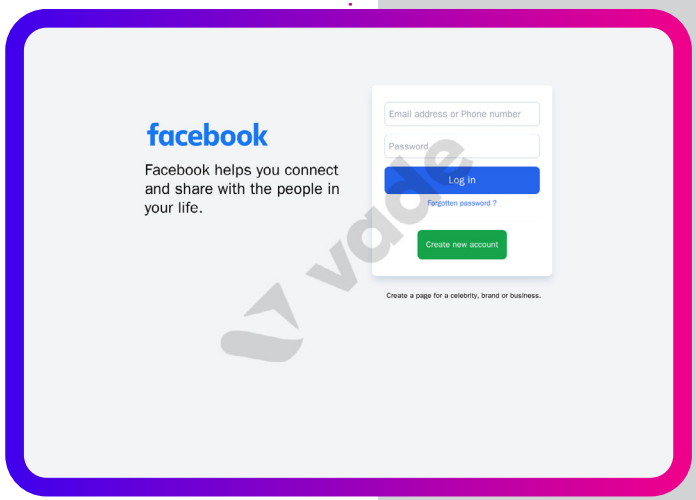
Dropped:
MTB, au, WellsFargo, Rakuten, Credit Saison, Adobe, Santander

SOCIAL MEDIA PHISHING REACHES A NEW LEVEL

Social media phishing has loomed as a top threat for organizations and consumers alike. This year's data only reinforced that reality, illustrating that it remains a favorite scam among phishers.

In a year when unique phishing URLs decreased for most industries, **social media saw volumes increase by more than 113% YoY**, with cloud the only other to experience an uptick (4%). Facebook clearly was responsible for social media's rise, yet Instagram, WhatsApp, and LinkedIn all contributed. Instagram ended the year as #9 on the list, followed by WhatsApp (#13) and LinkedIn (#23). Instagram and WhatsApp are no strangers to the top 20. Their inclusion continued a trend for the third straight year, while LinkedIn made appearances on the list in 2020 and 2021.

While platforms like Facebook and Instagram are often viewed as consumer-focused, it's important to remember they play an important role for businesses. Organizations of all sizes depend on these social media platforms for sales, marketing, recruiting, and hiring. A global survey of marketers found that nearly 90% use Facebook to promote their business, while 80% use Instagram for the same purpose.[1] Unsurprisingly, Facebook's global advertising revenue is forecasted to reach 127 billion (USD) by 2027, a new record after years of sustained growth.[2]



Facebook phishing page detected by Vade

Instagram phishing page detected by Vade

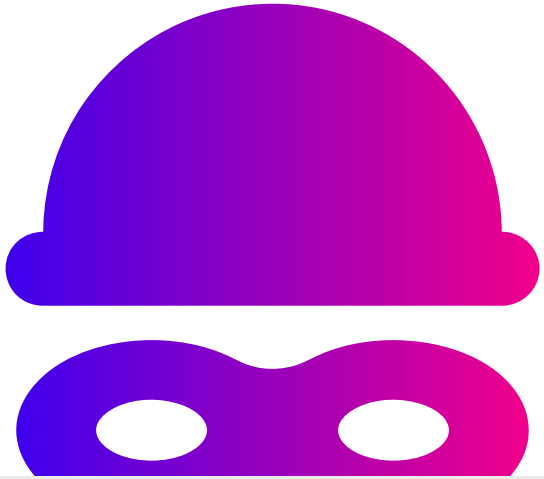
[1]Statista. "Leading social media platforms used by marketers worldwide as of January 2023." https://www.statista.com/statistics/259379/social-media-platforms-used-by-marketers-worldwide/

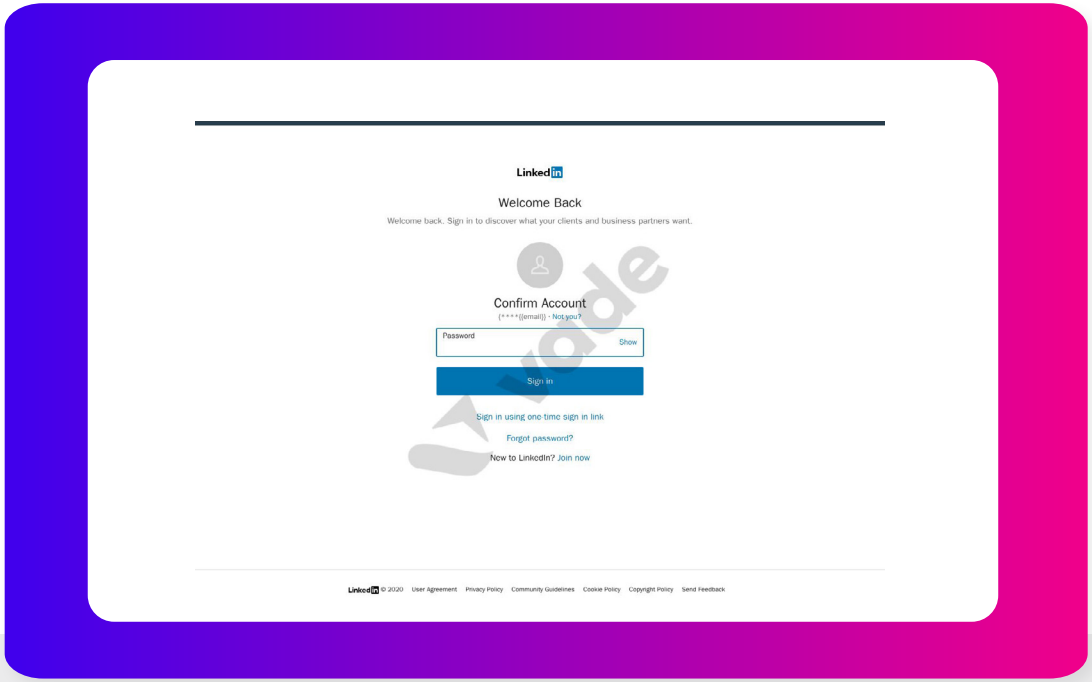
[2]Statista. "Advertising revenues generated by Facebook worldwide from 2017 to 2027." https://www.statista.com/statistics/544001/facebooks-advertising-revenue-worldwide-usa/

SOCIAL MEDIA PHISHING REACHES A NEW LEVEL

Meanwhile, LinkedIn remains a popular platform for business-to-business (B2B) sales and marketing, as well as talent management. Recent estimates suggest its ad revenue could nearly double between 2022 and 2027.[3]

Yet the incentive to impersonate social media brands goes beyond the importance of these platforms to consumers and organizations. Compromising social media accounts offers the opportunity to gain unauthorized access to other business applications. Recent reports show that more than 50% of workers globally reuse the same password for all work accounts.[4] And for small-to-midsized businesses (SMBs), this practice tends to be more prominent, as many lack formal security policies or personnel. This increases the risk of hackers using compromised credentials for social media accounts to gain unauthorized access to other important applications.





LinkedIn phishing page detected by Vade

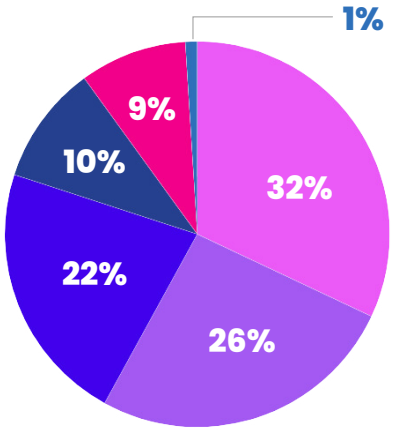
[3]Statista. "Annual advertising revenue generated by LinkedIn worldwide from 2017 to 2027." https://www.statista.com/statistics/275933/linkedins-advertising-revenue/
[4]TechReport. "Password Reuse Statistics: Over 60% Have a Password Problem." https://techreport.com/statistics/password-reuse-statistics/

THE FINANCIAL SERVICES INDUSTRY REMAINS THE MOST IMPERSONATED SECTOR, WITH SOCIAL MEDIA MAKING A LEAP

2023 proved to be another typical year for financial services, with the industry retaining its status as the most impersonated by hackers. The sector led all others in terms of total unique phishing URLs (64,009 or 32% of the overall total), followed by social media (51,183 or 26%), cloud (43,350 or 22%), Internet/telco (19,291 or 10%), e-commerce/logistics (17,882 or 9%), and government (1,903 or 1%). Notably, social media took second place for the first time since 2021, swapping positions with cloud. All other sectors finished in the same spot as the prior year.

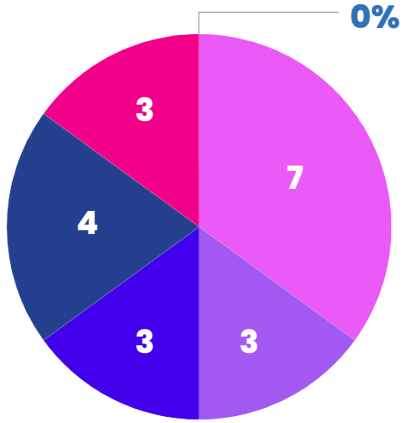
In terms of the top 20 most impersonated brands, financial services also led all industries. It featured the highest number (7), followed by Internet/telco (4), social media, cloud, and e-commerce/logistics (3), and government (0).

Phishing by Industry: 2023

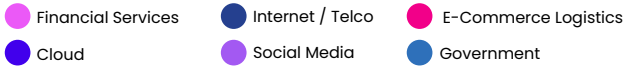


Percentage of phishing attacks by industry

Brands in Top 20: 2023



Number of brands by industry in top 20 of Phishers' Favorites

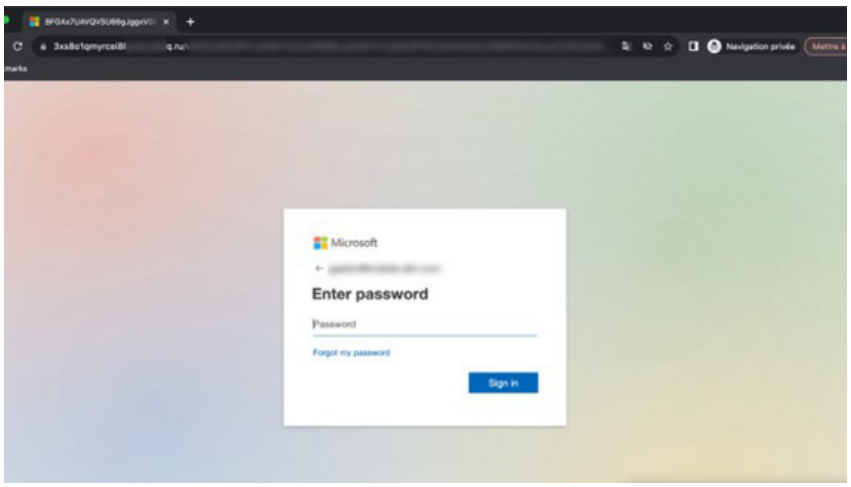


THE FINANCIAL SERVICES INDUSTRY REMAINS THE MOST IMPERSONATED SECTOR, WITH SOCIAL MEDIA MAKING A LEAP

These findings illustrate that impersonation attempts in financial services remain relatively distributed among a collection of brands. Meanwhile, spoofing in social media and cloud continues to be concentrated on a handful of companies. Cloud's popularity among phishers, for example, is concentrated on Microsoft, Google, and Netflix.

Financial services' dominance as the top spoofed sector comes as no surprise. Phishing attacks often aim to accomplish the short-term objective of gaining unauthorized access to a victim's account. The industry deals with the types of accounts that offer hackers the most lucrative payout, and this makes it very attractive to hackers.

The popularity of social media and cloud are also easy to understand. Social media was covered earlier; it's an easy avenue to harvest credentials or execute other schemes. But for cloud, we can look to the continued growth of collaboration suites like Microsoft 365 and Google Workspace for answers—not to mention their respective producers, Microsoft and Google.



Microsoft impersonation

THE FINANCIAL SERVICES INDUSTRY REMAINS THE MOST IMPERSONATED SECTOR, WITH SOCIAL MEDIA MAKING A LEAP

Microsoft 365, the most popular collaboration suite in the world, announced that it reached more than 382 million paid seats in Q3 2023.[5] That was a marked increase from the 258 million it reached during the same period in 2020.[6] Meanwhile, Google announced this year that more than 9 million organizations pay for Google Workspace.[7] Those executing phishing schemes go where there are users to exploit—and both Microsoft and Google have massive amounts of users.

Businesses rely on these platforms for every aspect of their operations. Users depend on them to communicate, collaborate, and produce—all in a fully and seamlessly integrated environment. That makes these digital suites top targets for hackers. A single compromise can open the door to a seemingly endless list of opportunities to exploit an organization, its customers, suppliers, and users.

[5]Microsoft. "Microsoft Fiscal Year 2023 Third Quarter Earnings Conference Call." https://www.microsoft.com/en-us/Investor/events/FY-2023/earnings-fy-2023-q3.aspx

[6]Microsoft. "Microsoft Fiscal Year 2020 Third Quarter Earnings Conference Call." https://www.microsoft.com/en-us/Investor/events/FY-2020/earnings-fy-2020-q3.aspx

[7]Business Insider. "Google Workspace, an office-software suite, hits 9 million paying organizations." hhttps://www.businessinsider.com/google-workspace-9-million-paying-organizations-2023-3

MOST IMPERSONATED BRAND BY INDUSTRY

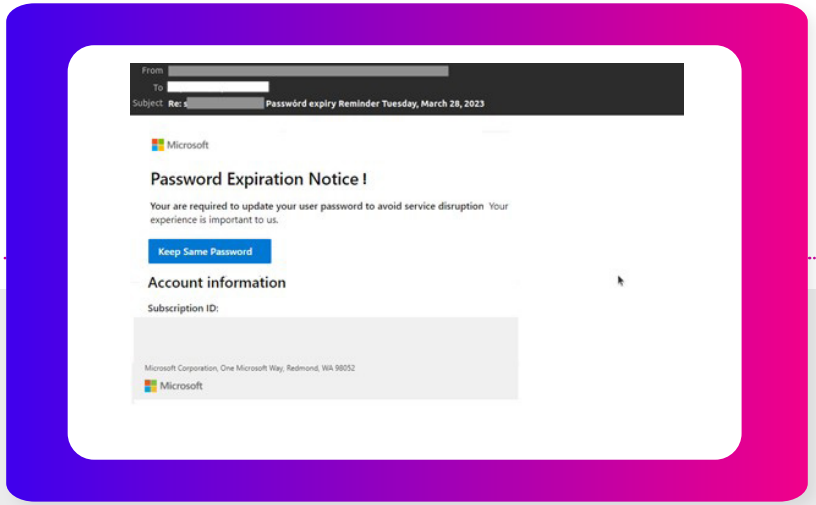
Brand	Category	Unique Phishing URLs
Facebook	Social Media	**44,548**
Microsoft	Cloud	**22,851**
Crédit Agricole	Financial Services	**11,668**
Orange	Internet/Telco	**8,719**
SoftBank	E-commerce/logistics	**4,522**
Impots	Government	**336**
		92,644

HACKERS ABUSE LEGITIMATE SERVICES

For hackers, 2023 continued the tried-and-true tactic of abusing legitimate services. We saw hackers exploit multiple popular brands—such as YouTube, Google, Baidu, and Cloudflare, to name a few. And the reasons are clear. Each platform provides significant value to consumers and businesses. Google, Baidu, and YouTube enable consumers and employees to find the information and services they need, and businesses to market and sell their products and services. Meanwhile, Cloudflare enables organizations to provide an optimal and secure online experience, and users to benefit from it. One reality hasn't changed. The more valuable the service, the more incentive hackers find in exploiting it.

In April, hackers targeted Microsoft 365 users with an attack that used YouTube as a way to bypass filters blocking their malicious links. Intended victims of the attack received a spoofed email alerting them that their Microsoft 365 password has expired and calling for them to update it.

The email contains a phishing URL, yet hackers have rewritten the link using YouTube's attribution link feature (used to give credit to creators when their work is reused). When users click the rewritten link, thinking it's the password reset link, they visit YouTube temporarily before being directed to the original URL. This tactic is very attractive to hackers, as it allows them to hide phishing links behind YouTube's high-authority domain, which circumvents detection by email filters relying on reputation-based detection.

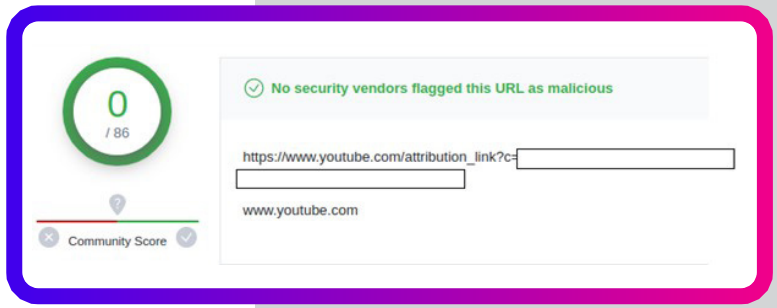


Phishing email impersonating Microsoft 365

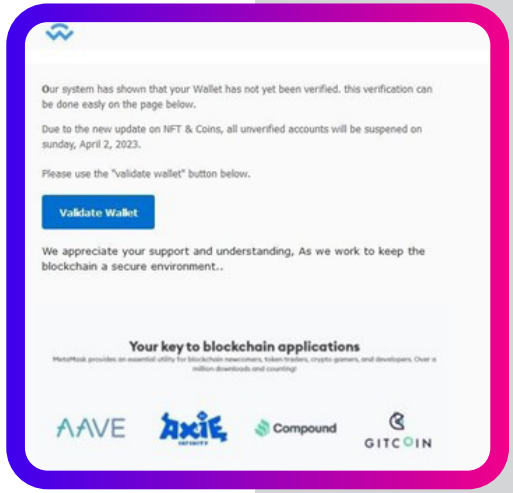
While hackers have used YouTube redirect URLs in phishing attacks before this, the use of YouTube attribution links is a new tactic that could bypass email filters that scan for suspicious redirects. Unsurprisingly, no security vendors outside of Vade viewed the phishing URL as malicious, according to VirusTotal.

It wouldn't be a Phishers' Favorites report without a cryptocurrency scam!

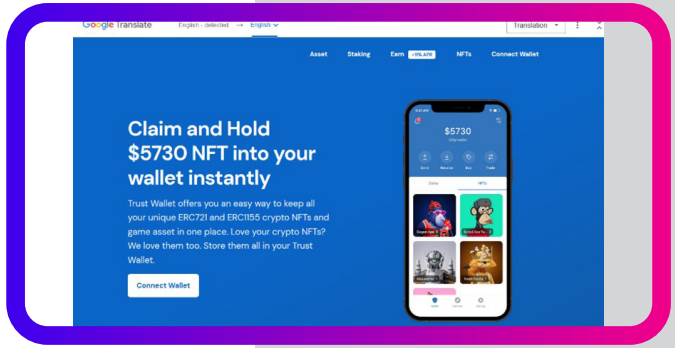
In a similar attack, Vade analysts uncovered a threat targeting users of Wallet Connect, a cryptocurrency wallet. Like most phishing emails, the attack creates a sense of urgency, warning users that their cryptocurrency wallet would be suspended if they don't validate their wallet. This is a social engineering tactic designed to elicit an emotional response from the victim and compel them to take a compromising action.



VirusTotal query of malicious URL



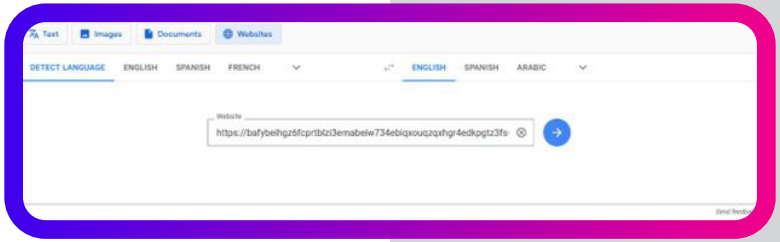
Phishing email impersonating Connect Wallet



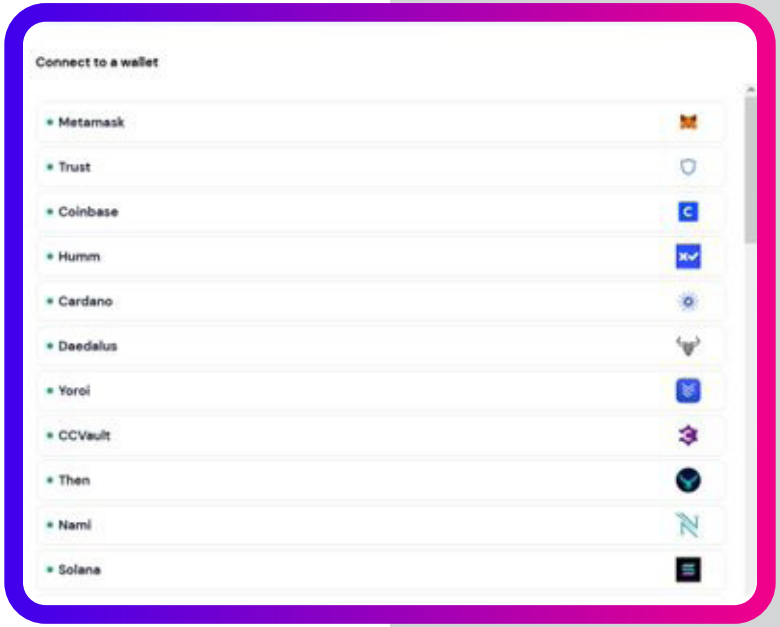
Facebook phishing page detected by Vade

In this case, the hackers use Google Translate to rewrite their malicious URL with the service's high-authority domain. This attack also leverages IPFS Decentralized Network to host a phishing kit. IPFS is a decentralized storage and delivery network based on peer-to-peer (P2P) networking that enables users around the world to exchange files. It's an attractive target for cybercriminals because it provides free file storage and only owners of a file uploaded to IPFS can remove it from the system. Victims can also open the file without running an IPFS client on their devices.

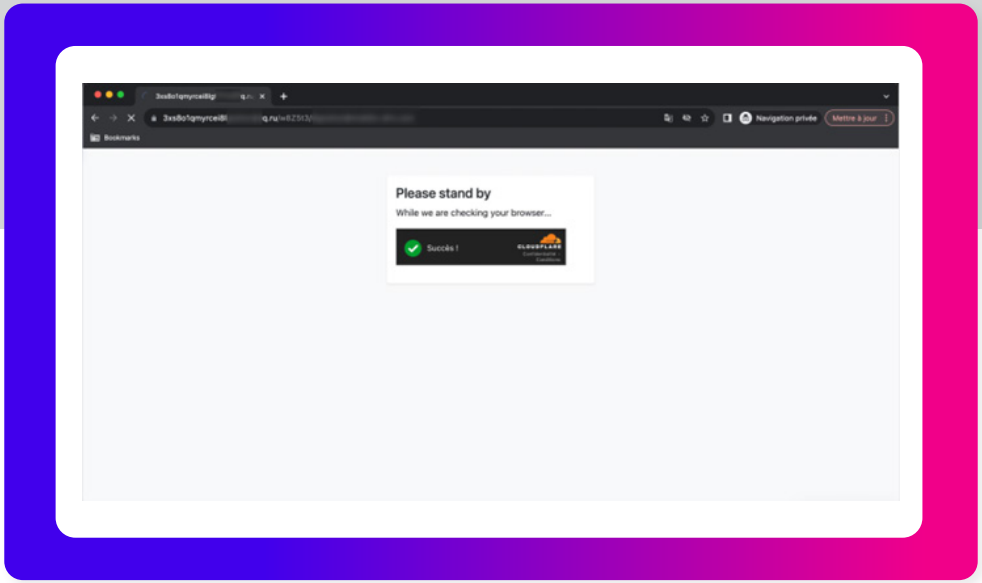
Additionally, the attack also uses JavaScript and CSS obfuscation techniques to determine what content to display to the victim and when, simulating an experience that appears legitimate on a desktop or mobile device. Designed to ultimately steal the victim's credentials and takeover their cryptocurrency account, the simulation allows victims to connect up to 21 spoofed cryptocurrency wallets. Victims are then prompted to enter their Recovery Phrase, Keystore JSON, and Private key, which hackers harvest upon entry.



Malicious link rewritten with Google Translate



Fake window listing cryptocurrency wallets



Cloudflare antibot mechanism

While link redirects were a common feature of phishing attacks in 2023, so was the abuse of Cloudflare. In one attack, hackers targeted Microsoft 365 users and leveraged the redirect link feature of Baidu, China's most popular Internet search engine.

The phishing email contains a phishing link disguised as a Baidu domain. The link directs victims to a Baidu webpage before sending them to an intermediary page. Here, the page simulates a Cloudflare security check. The phishing page is hosted on Cloudflare and thus benefits from the platform's antibot mechanism. The mechanism mimics human behavior and enables threats to bypass automated bot detection solutions.

From Cloudflare to Google and other global brands, the abuse of legitimate services proved innovative and effective. In many cases, the techniques evaded detection from most security vendors, as reported by VirusTotal.

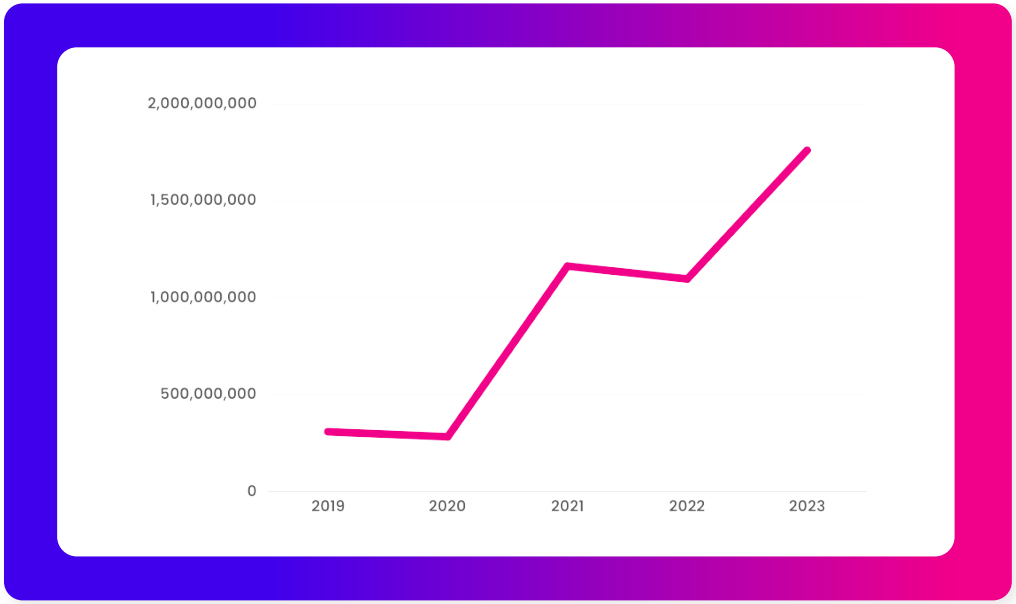
QUISHING MAKES A COMEBACK—AND WITH A VENGEANCE

Quishing, or QR code phishing, isn't a new threat, but it has captured headlines as of late. In quishing attacks, hackers embed a phishing URL in the QR code to make it harder for email filters to detect. While Vade first detected the threat as early as 2017, we observed an alarming increase in quishing attacks in Q2, which continued for the remainder of the year.

Quishing email impersonating Microsoft

And the reasons are clear. Despite being a well-established threat, some email security filters still lack QR code reading capabilities, preventing them from seeing and analyzing a malicious URL. At the same time, quishing can present challenges for more advanced email security solutions that use Computer Vision. Computer Vision is a type of AI algorithm that can extract malicious links embedded in QR codes. According to Sebastien Goutal, Vade's Chief Science Officer, scanning a high volume of QR codes with Computer Vision requires significant memory and processing power and slows down the processing of emails. Some email security solutions overcome this limitation by analyzing other email features before using Computer Vision. These solutions are in the minority, however.

This could help explain why hackers are sending more phishing emails than ever before. Looking at the past few years, we see a marked trend upward, with volumes reaching their highest level in 2023 since Vade started keeping track in 2015.



Phishing emails detected by Vade since 2019

“SCAMA”: UNEARTHING THE DARK MARKETPLACE

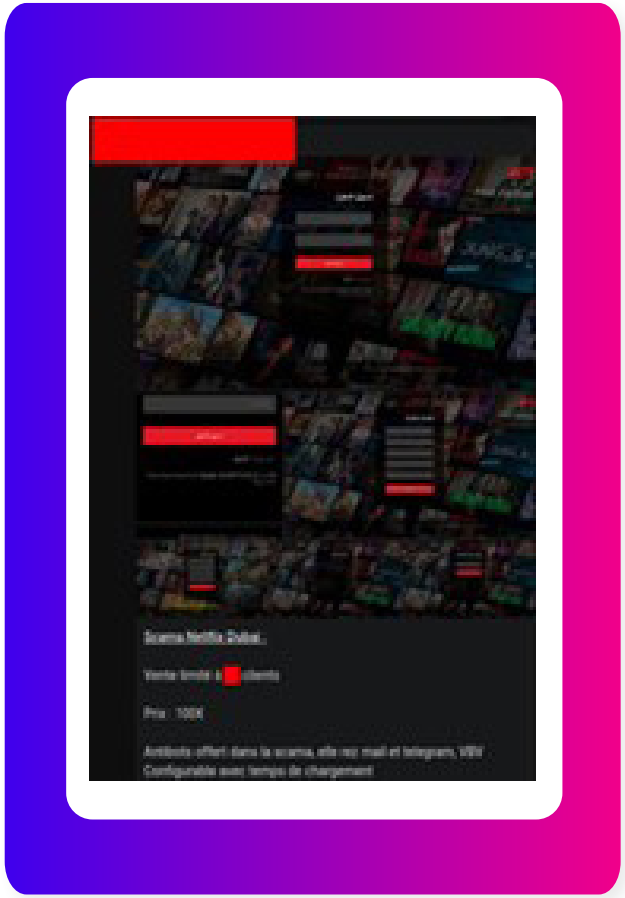
Speaking of productivity, phishing kits are a key reason for the increased volume of phishing attacks. Not only do they eliminate most of the legwork of designing, developing, and deploying an attack, but they also lower the barriers to entry for anyone with aspirations of becoming a cybercriminal.

In 2023, Vade analysts revealed an in-depth analysis of scama—another term for phishing kits and a reference to the dark, nefarious marketplace for buying and selling them. The malicious industry exists on platforms like Telegram, where cybercriminals exchange everything needed to launch an advanced phishing campaign. This includes email templates and webpages spoofing legitimate brands and services.

Scama are sold in packs and often primarily hosted in the Asia-Pacific region on relatively well-known web hosting platforms—enabling hackers to avoid stringent data protection laws and international extradition agreements.

These packs are also advertised and marketed like any other product, with Telegram posts listing features like “anti-bot protection” and responsive design for mobile and desktop use.

Hackers continue to innovate and introduce new phishing kits that can evade detection and adapt to any location in the world. This highlights the importance of adopting an email security solution that protects against emerging threats that have yet to surface.



Netflix Dubai scama pack sold on Telegram

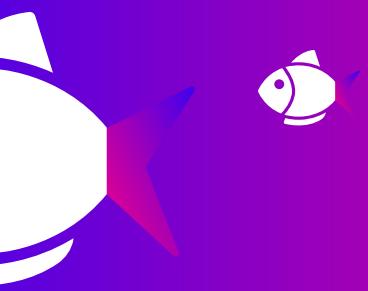
PHISHING ATTACKS: DYNAMIC THREATS CALL FOR MULTI-LAYERED PROTECTION

Phishing remains a top cyberthreat for organizations. No other attack method remains as popular or prolific in exploiting victims, as threats continue to become more frequent and sophisticated. For businesses, staying protected calls for a multi-layered approach that fortifies the vulnerabilities in your attack surface. To protect against today's most sophisticated phishing threats, look to adopt the following measures:

• **Advanced, integrated email security:** Since 2020, Gartner has recommended that organizations protect their cloud-based email with an integrated, third-party solution.[8] In 2023, they reiterated this recommendation. Only an integrated, third-party email security solution can defend against emerging phishing threats, including those known as "zero-day." For this level of protection, look for solutions that leverage machine learning, natural language processing, and computer vision algorithms. Together, they provide predictive defense against all types of phishing threats, including text- and image-based threats. Also, favor solutions that incorporate human insights, utilize real-time global threat intelligence, and offer robust features for threat prevention, detection, and response. The combination better equips you to monitor for and protect against advanced phishing attacks.

• **Robust and unified incident response**: Security incidents are an inevitable reality in cybersecurity. When they happen, responding with speed and precision matters. Look for technology that automatically remediates email threats across your tenants or users, allows you to triage and remediate user-reported emails, and enables you to manage cybersecurity from a central location.

[8]Gartner. "Market Guide for Email Security." https://www.gartner.com/en/documents/3989940



• **Extended protection from mailbox-to-browser**: While email is the top attack vector, often the payload is delivered via the web. Protect your mobile and desktop users with a remote browser isolation (RBI) solution. RBI technology safeguards users from browser attacks by launching a remotely hosted session for every browsing session. For optimal email security, look for solutions that extend this protection from email links to the web, while also allowing you to seamlessly control whitelists.

• **Phishing awareness training**: Human error remains the leading cause of data breaches.[9] Users seem particularly susceptible to interacting with malicious links and attachments. Phishing awareness training attempts to solve this vulnerability, teaching users to identify potential threats and report them to administrators for remediation. While any form of training can help, look for programs that administer electronically, automatically, on-demand, and according to each user's role and seniority. These features provide the best results and ensure the training reflects the threats each user is likely to encounter.

[9]Verizon. "2023 Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/dbir/

About Vade

Vade is a leading cybersecurity firm specializing in AI-driven threat detection and response solutions for Microsoft collaboration suite, with a focus on serving Small to Medium-sized Businesses (SMBs) and their Managed Service Providers (MSPs). With a global presence across eight locations, including the United States, France, Japan, Canada, and Israel, Vade's flagship product, Vade for Microsoft 365, seamlessly provides supplementary cybersecurity services for Microsoft's collaboration suite. The company's best-in-class security solutions integrate robust AI-driven protection and automated threat remediation, resulting in improved efficiency, reduced administrative overhead, and optimized cybersecurity investments.

Vade provides distinctive protection against phishing, spear phishing, and malware, ensuring error-free configurations and enabling rapid deployment. Vade is a trusted choice for some of the world's leading internet service providers and security solution providers, ensuring the security of 1.4 billion email inboxes.

vade

Subscribe to our blog:

www.vadesecure.com/en/blog

Follow us :

@vadesecure