

Email Phishing and DMARC Statistics: 2026 Security Trends

A practical look at phishing growth, real-world attack patterns, and how DMARC reduces domain-based abuse.



EMAIL PHISHING AND DMARC STATISTICS

Download for free

Key Takeaways



Phishing has evolved into one of the easiest entry points for attackers, growing from hundreds of thousands of attacks in 2016 to **millions of attacks every month by 2023–2025**



The **average cost of a phishing-related breach reached approximately \$4.88 million in 2025**



Phishing thrives because it targets people, not systems, and scales easily through automation and AI



Email spoofing remains a core tactic behind successful phishing campaigns



DMARC significantly reduces spoofing risk, but adoption and enforcement remain uneven worldwide



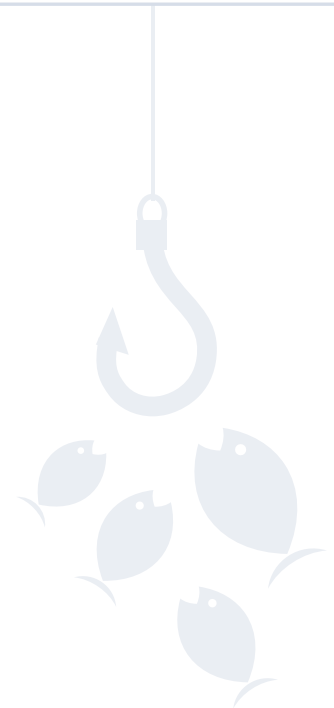
Introduction



Email phishing remains one of the most effective and damaging methods of cyberattack. By impersonating trusted brands, employees, or service providers, attackers bypass technical controls and exploit human trust. This approach continues to result in billions of dollars in annual losses due to fraud, data theft, operational disruptions, and reputational damage.

DMARC statistics consistently show that **email spoofing is one of the primary entry points for phishing campaigns**. When domains lack proper authentication and enforcement, attackers can send emails that appear legitimate, even though they originate from unauthorized sources.

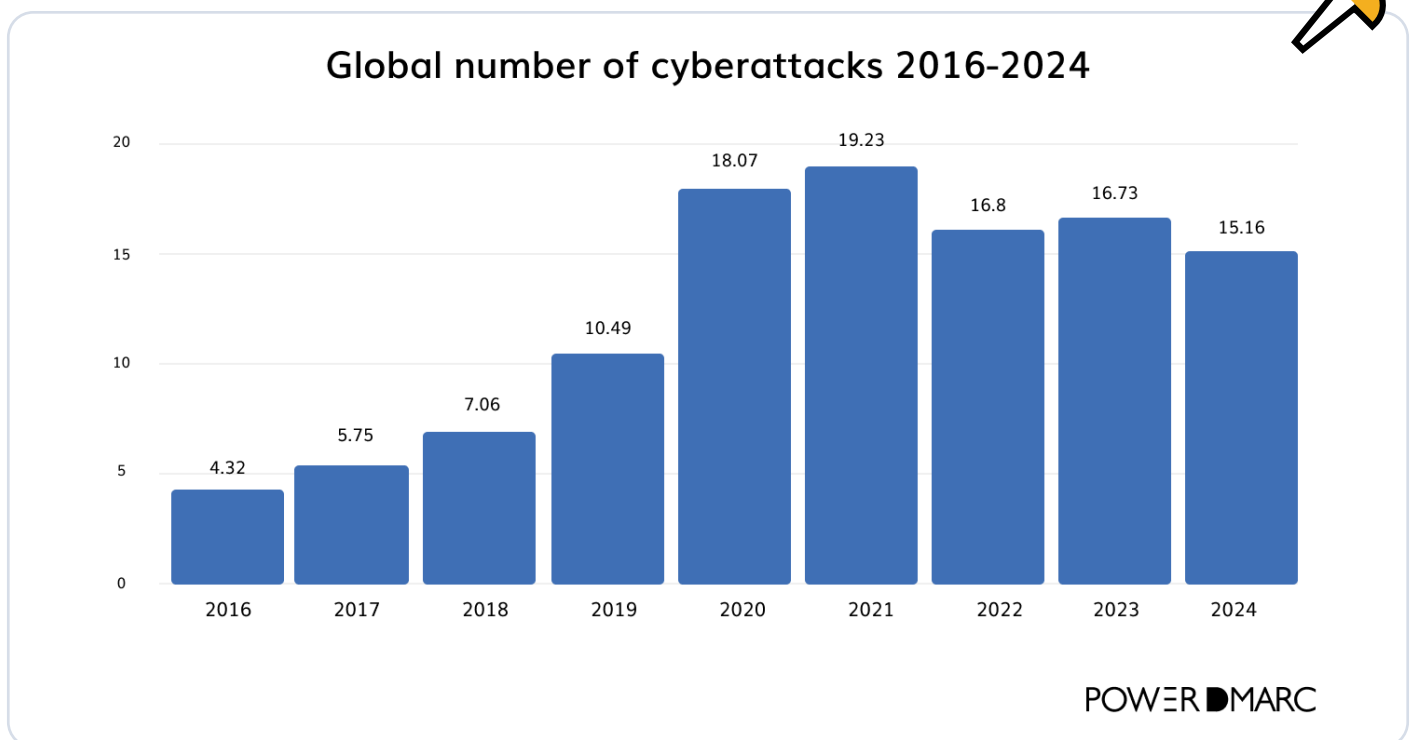
To address this risk, organizations increasingly rely on email authentication standards such as SPF, DKIM, and DMARC. Among these, DMARC plays a central role by tying authentication results to policy enforcement and visibility, allowing domain owners to prevent spoofed emails from reaching inboxes.



Key Cybercrime Statistics

Cybercrime activity continues to grow in both volume and sophistication. In 2016, approximately **4.3 million cyberattacks** were reported globally. By 2021, that number had increased to **over 19 million**, driven in part by rapid digitalization and pandemic-era shifts to online work.

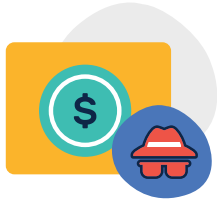
The trend remains concerning. In the first half of 2025 alone, **more than 8,000 data breaches exposed roughly 345 million records**, demonstrating how persistent and large-scale cyber threats have become.



AI is now accelerating this problem. According to Experian's 2026 Data Breach Industry Forecast, artificial intelligence is enabling attackers to:

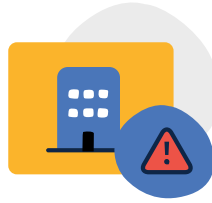
- ▶ Create convincing fake identities
- ▶ Automate attacks at scale
- ▶ Evade detection faster than traditional defenses can adapt

Top Cybercrime Categories by Impact



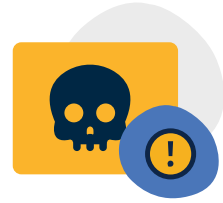
Investment fraud:

\$6.5 billion in losses, driven by social-engineering scams such as crypto fraud



Business email compromise (BEC):

\$2.9 billion in reported losses, exploiting trusted email workflows



Ransomware:

Average downtime of 24 days per incident in 2025, with operational costs often exceeding ransom demands

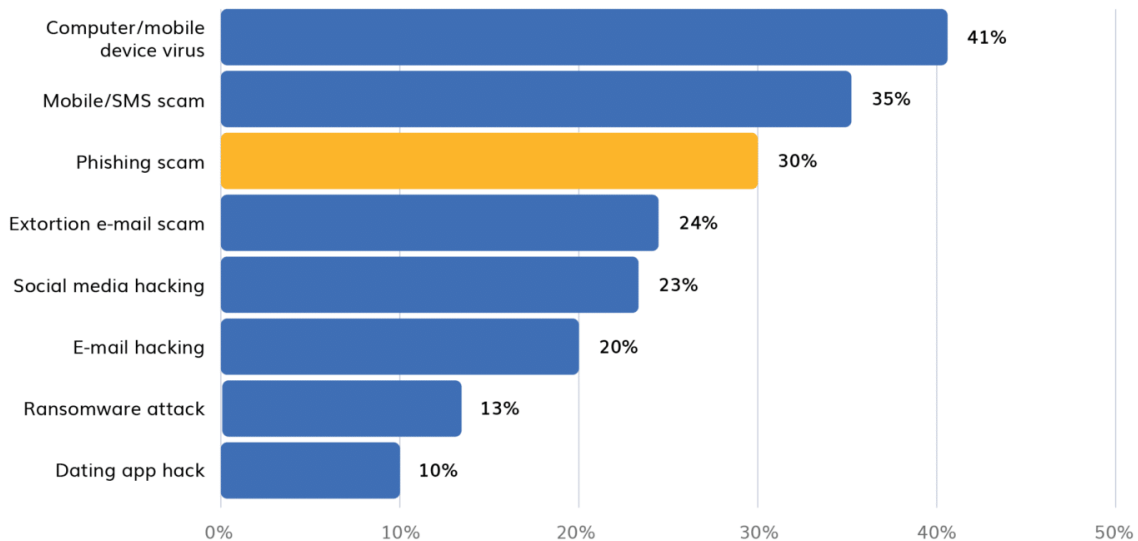
These patterns indicate that cybercrime continues to evolve in tandem with technological advancements, with email remaining a primary attack vector.

Phishing and Data Breaches

Phishing Scams

Phishing attacks increased sharply during the pandemic, rising from approximately **0.44 million incidents in 2016 to nearly 9 million by 2023**. In 2025, phishing remains one of the most damaging cyber threats, with an average breach cost of **\$4.88 million**.

Online adults experiencing cybercrime, by type



POWERDMARC

Phishing succeeds because attackers manage to:

- ▶ Steal login credentials
- ▶ Trigger follow-on attacks such as ransomware or account takeover
- ▶ Exploit trusted communication channels with minimal technical effort

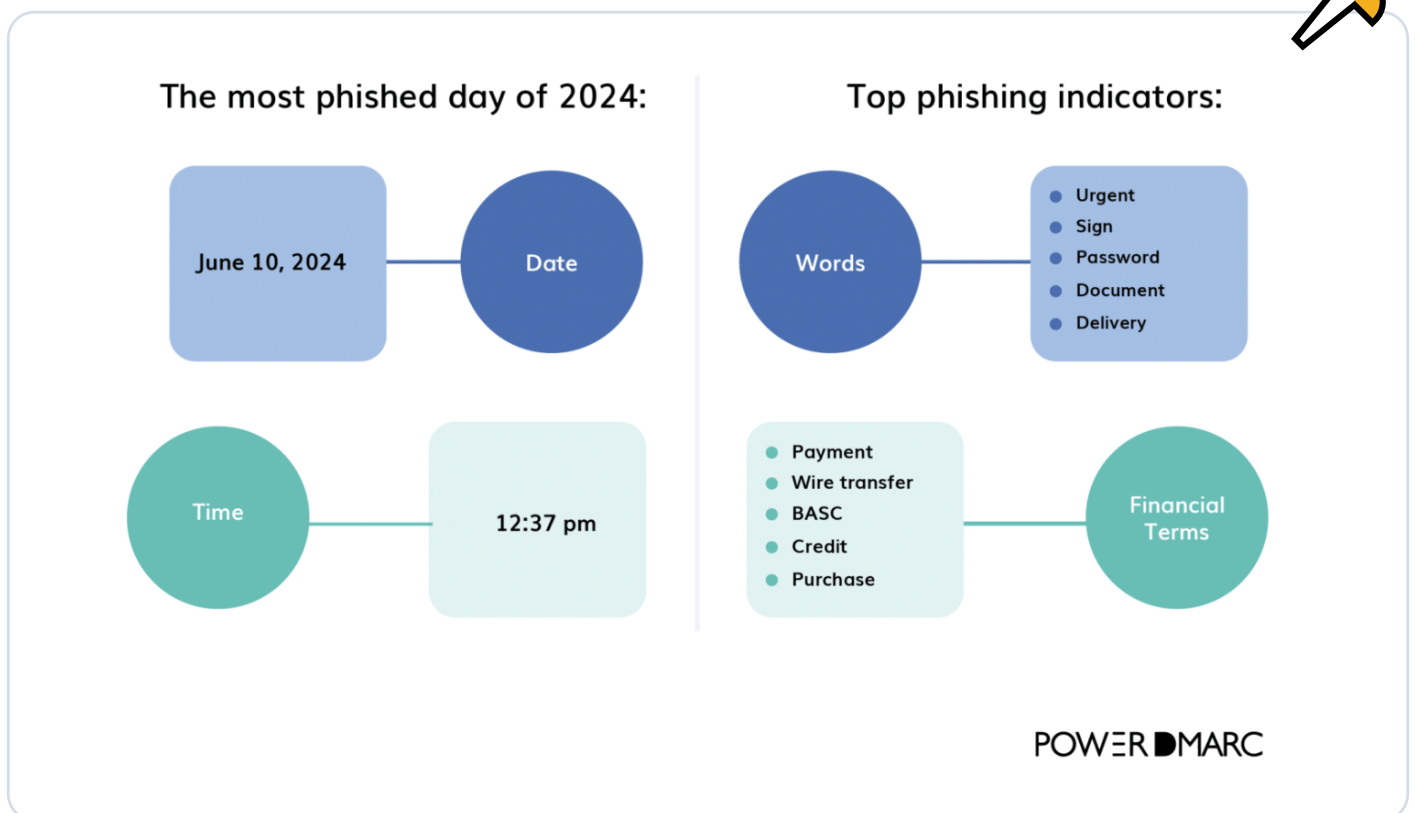
Personal Data Breaches

Personal data breaches ranked second globally, with **1.66 million incidents reported worldwide**. These breaches typically expose:

- ▶ Names and email addresses
- ▶ Login credentials
- ▶ Financial or medical data

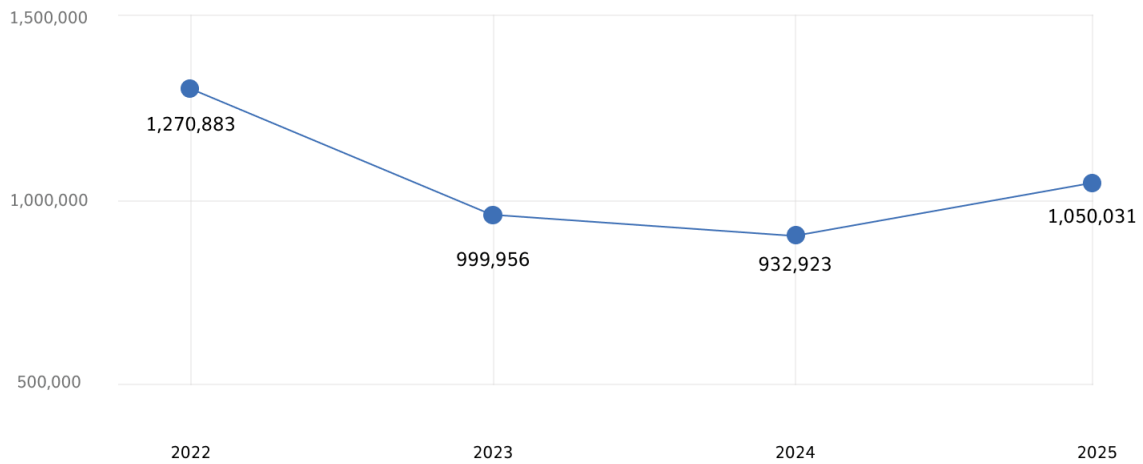
Other major categories included extortion, investment fraud, tech support scams, identity theft, and credit card fraud. Across all categories, the core pattern remains the same: data exposure followed by financial exploitation.

Phishing at Scale: Trends and Targets





Number of global phishing sites



POWERDMARC



Ranking of TLDs Used by Phishing Sites in 2025: Top 10

- 1 .com
- 2 .top
- 3 .xin
- 4 .xyz
- 5 .bond
- 6 .vip
- 7 .info
- 8 .online
- 9 .ru
- 10 .pro

POWERDMARC

“ Phishing is no longer cyclical. It is a persistent, high-volume threat that organizations must manage continuously. ”

Cybercrime Statistics

United States



In the United States, phishing and spoofing were the most frequently reported cybercrime categories in 2024, according to the FBI's Internet Crime Complaint Center (IC3).

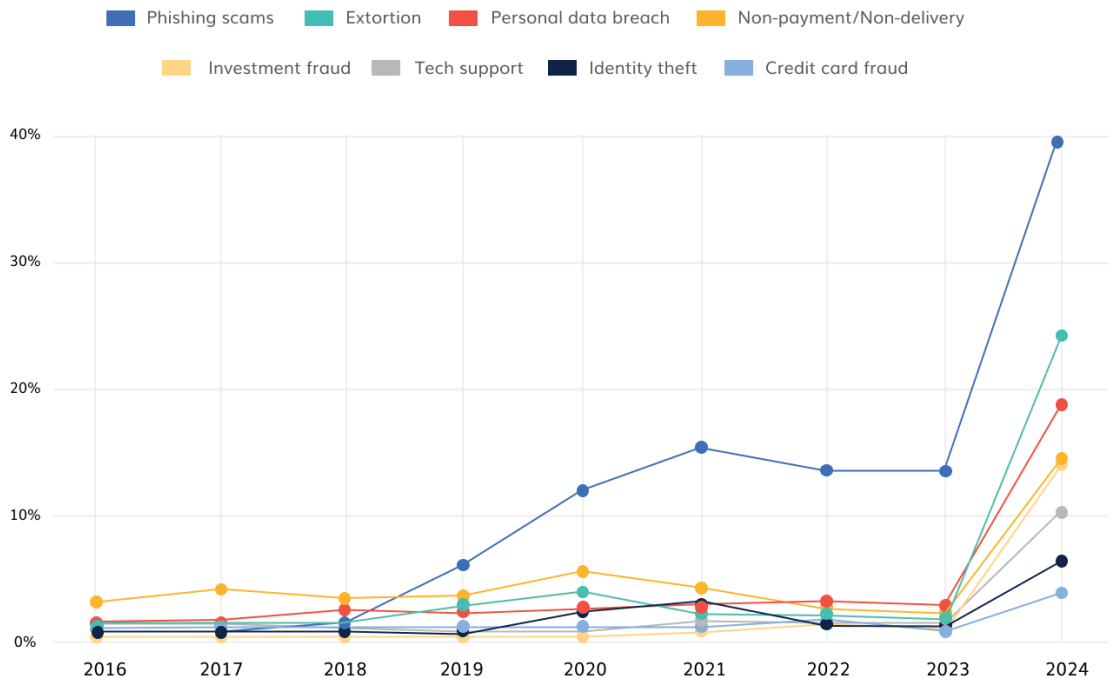
Other common types of cybercrime:

- ▶ Personal data breaches
- ▶ Tech support fraud
- ▶ Non-payment/non-delivery scams
- ▶ Extortion

Worldwide



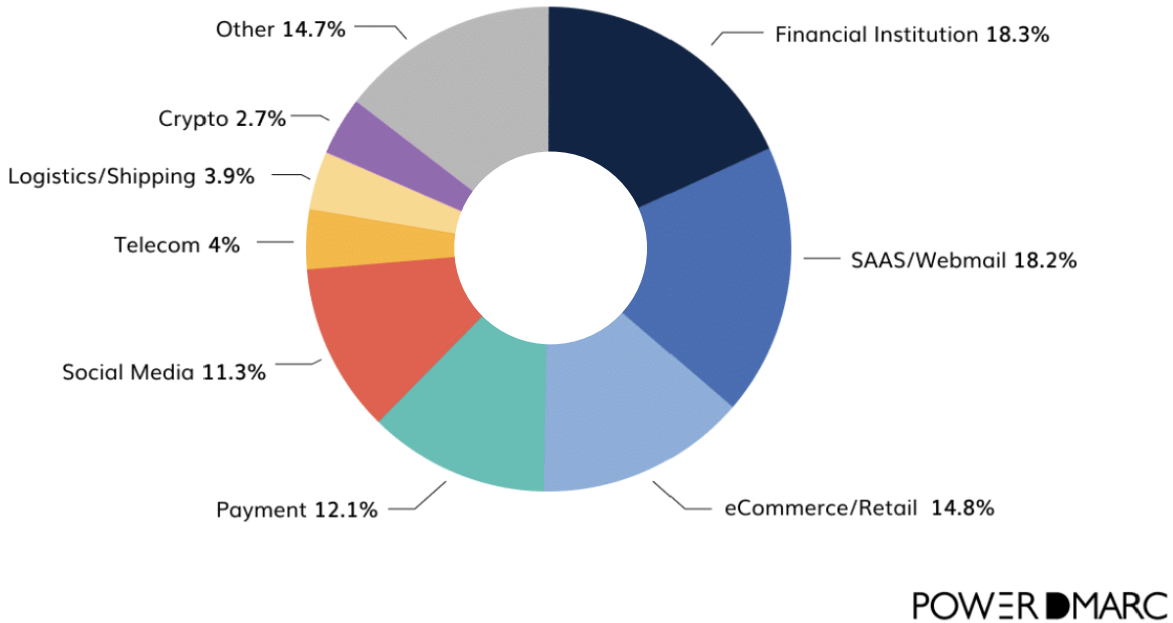
Global number of cyberattacks 2016-2024, by type (in millions)



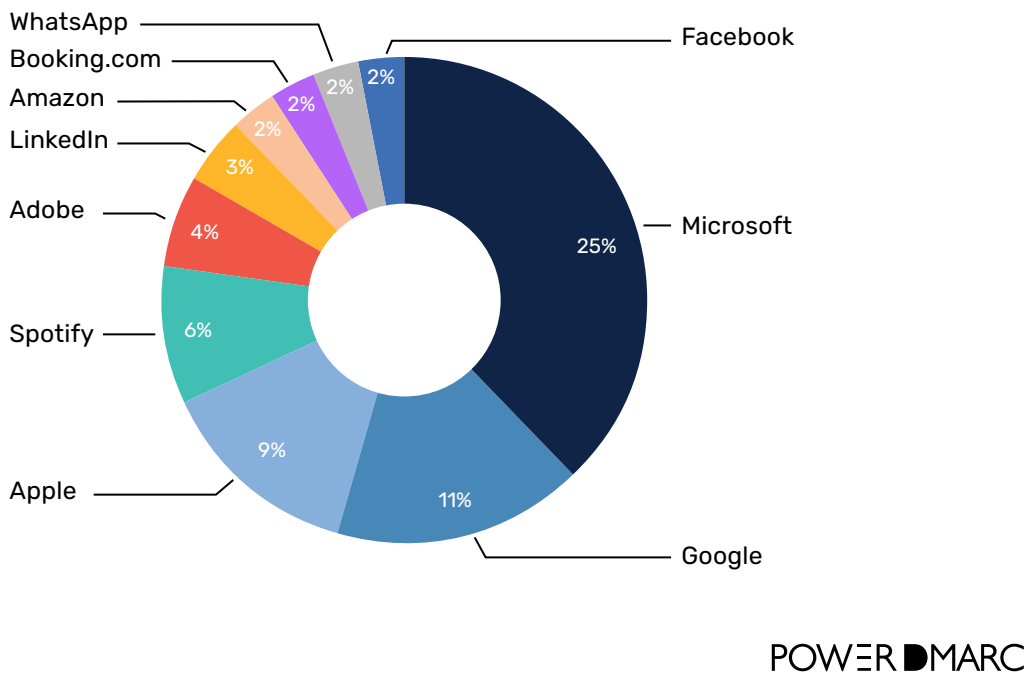
POWERDMARC

Who and What Attackers Target

Industries Most Targeted

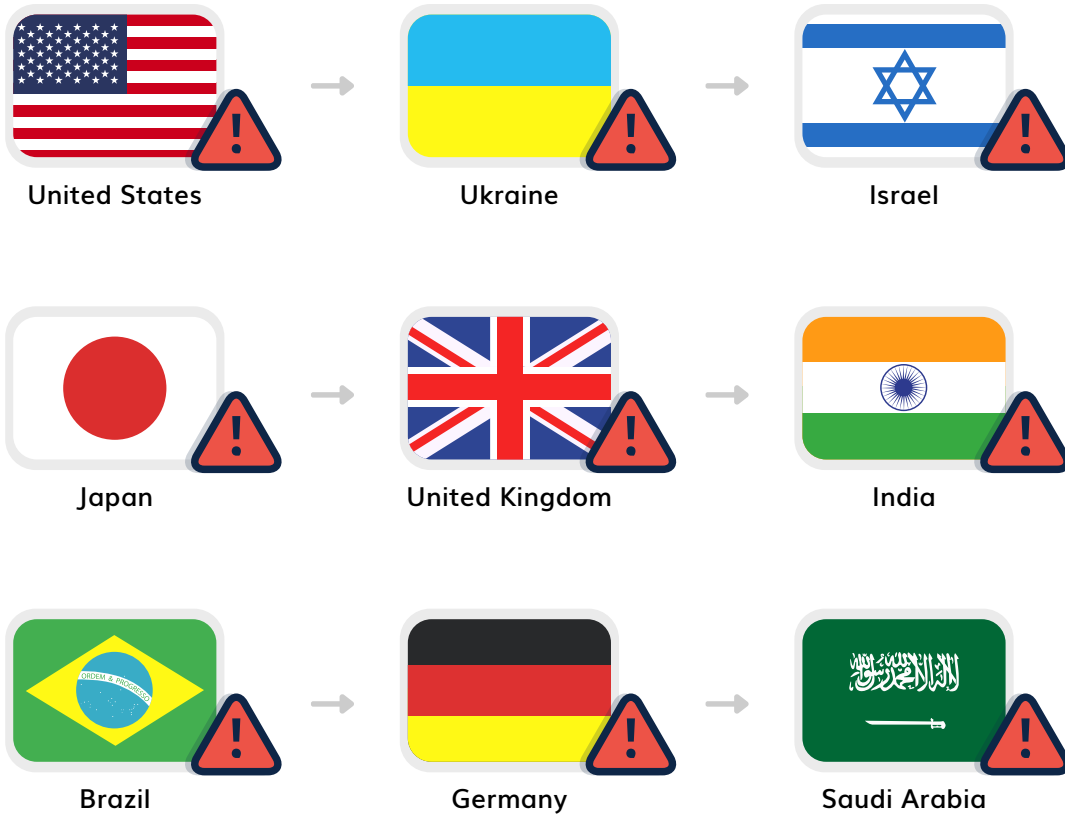


Most Targeted Brands (Q2 2025)



Attackers increasingly focus on account-based platforms rather than retail brands, aiming to steal credentials and enable broader fraud.

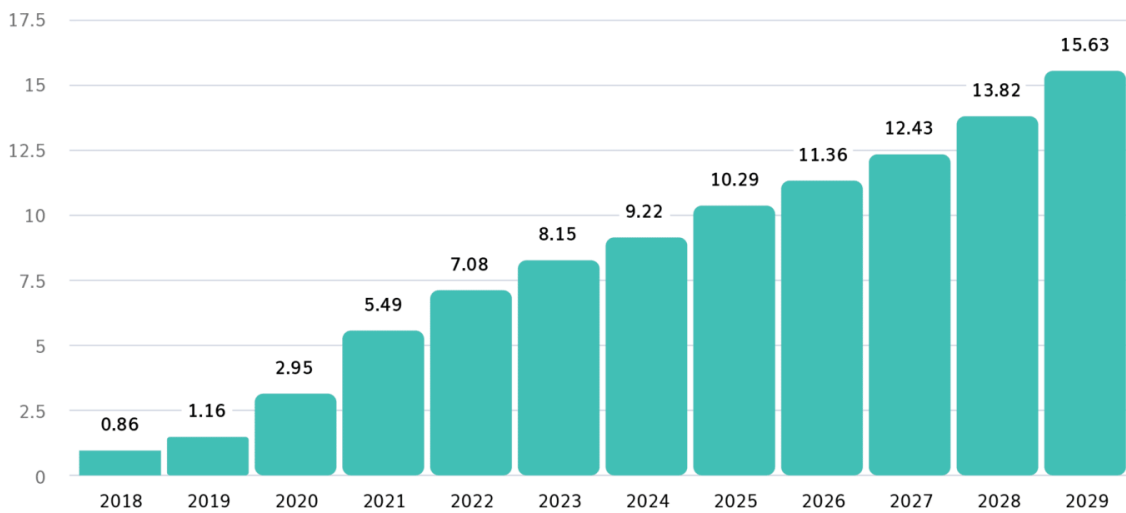
Most Targeted Countries of 2025



The Cost and Impact of Cybercrime



Annual Estimated & Predicted Cost of Cybercrime Worldwide



POWERDMARC

Major incidents in early 2025 highlighted how exposed organizations remain:

- ▶ Coupang breach affecting 33 million customers
- ▶ 700Credit API breach exposing 5.8 million records
- ▶ Oracle EBS zero-day exploitation
- ▶ Salesforce/Gainsight supply-chain compromise
- ▶ Qantas data leak involving 5 million customers

These incidents show how single points of failure, third-party risk, and weak email security can create large-scale consequences.

DMARC Statistics and Adoption Gaps











DMARC has become a critical control as mailbox providers tighten authentication requirements. Google and Yahoo now require DMARC for bulk senders, contributing to a **65% reduction in unauthenticated email reaching Gmail inboxes.**

Adoption by Industry

- ▶ Banking shows relatively strong adoption, but still falls short of full coverage
- ▶ Insurance and legal services hover around 52% adoption
- ▶ Aviation, software, and financial services cluster near 45%
- ▶ Enforcement remains the biggest gap across all sectors

The data is consistent: adoption without enforcement delivers limited protection.

2025 Country-Level DMARC Research By PowerDMARC

Country	Cyber Risk Context	DMARC Adoption Snapshot	Key Exposure / Gap
 Norway	Rising phishing and social-engineering fraud, especially financial scams and identity theft	Near-universal adoption in finance (only 6.8% without DMARC); healthcare leads enforcement (55.6% p=reject)	Transport lags (28.8% no DMARC; 9.1% reject); weak MTA-STS and moderate DNSSEC
 Morocco	High malware and banking-trojan activity; repeated attacks on media and public institutions	Insurance shows higher adoption (66.67%); most sectors far lower	Minimal enforcement (11.11% reject in insurance); several sectors have 0% reject
 Tunisia	Growing attacks on government and industrial sectors; rising fraud losses	Education leads adoption (42.62%); finance and telecom ~33%	Government weak (18.39% DMARC); no transport-layer or DNS reinforcement
 Netherlands	Sophisticated state-linked threats; NIS2 pressure increasing	Government strong (~1% without DMARC); healthcare and education above average	Transport and telecom exposed (~65% without DMARC); uneven sector protection
 Sweden	Increased ransomware and extortion activity; high digital exposure	Banking leads (~84% adoption); overall relatively high coverage	Media and telecom lag; limited transport and DNS protections
 Peru	Rapid rise in phishing, ransomware, and impersonation attacks	~67% of domains publish DMARC	Healthcare (37% no DMARC), telecom (43% no DMARC), transport (36% no DMARC)
 Belgium	Persistent impersonation risk due to EU, finance, and government targeting	Majority adopted DMARC; 20.6% still uncovered	Government (26% no DMARC) and transport (36% no DMARC) remain exposed
 New Zealand	Growing phishing against public-sector domains; reforms underway	Government relatively strong (13% no DMARC)	Transport (52% no DMARC); ~37% of domains nationally unprotected
 Italy	Ongoing phishing-driven financial losses across critical sectors	~74% adoption overall	Government, healthcare, transport, telecom each show 25–33% gaps
 Germany	Email-based fraud and espionage targeting critical infrastructure	Majority publish DMARC; 32.3% lack DMARC	Government (42% no DMARC); healthcare (53% no DMARC)

Why DMARC Enforcement Matters

Countries and organizations that move beyond monitoring and actively enforce DMARC see measurable security gains:

- ▶ Fewer successful spoofing attempts
- ▶ Improved sender reputation
- ▶ Better inbox placement for legitimate email

By contrast, domains that leave DMARC in "p=none" mode continue to experience brand abuse despite having SPF and DKIM in place.

Manual DMARC implementation remains a challenge due to:

- ▶ DNS complexity
- ▶ Unreadable XML reports
- ▶ Risk of misconfiguration

Managed DMARC platforms address these barriers by automating setup, monitoring, and enforcement, allowing organizations to protect their domains without operational friction.

Final Takeaway

Phishing is not slowing down. As attackers scale with AI, **email trust must be enforced, not assumed**. DMARC, when properly implemented and enforced, remains one of the most effective controls for reducing phishing risk at the domain level.



For organizations looking to implement or strengthen DMARC, the challenge is often operational: DNS complexity, unreadable reports, and the risk of blocking legitimate mail. This is where managed DMARC platforms come in.

PowerDMARC: The Best DMARC Provider

PowerDMARC is an email authentication and domain security platform that helps organizations protect their domains from phishing, spoofing, and email-based fraud.

What does PowerDMARC do?




PowerDMARC simplifies and automates email authentication by:

- ▶ Managing DMARC, SPF, DKIM, BIMI, MTA-STS, and TLS-RPT
- ▶ Providing clear visibility into who is sending emails on your behalf
- ▶ Helping you block unauthorized senders
- ▶ Improving email deliverability
- ▶ Helping businesses stay compliant with global security standards.






How PowerDMARC Helps Reduce Phishing and Domain Abuse




Complete DMARC Visibility

-  Converts complex DMARC XML reports into clear, actionable dashboards
-  Identifies authorized vs. unauthorized sending sources
-  Detects spoofing, impersonation, and misaligned email traffic in real time




Safe DMARC Enforcement

-  Guided transition from monitoring (**p=none**) to full protection (**quarantine / reject**)
-  Minimizes false positives and delivery disruption
-  Improves sender reputation with mailbox providers

Protection Against Brand Impersonation

-  Blocks unauthenticated emails before they reach inboxes
-  Reduces phishing attacks using spoofed or look-alike domains
-  Protects customer, partner, and internal communications

Built for Modern Email Requirements

-  Supports Google and Yahoo bulk sender requirements
-  Helps maintain spam complaint thresholds and authentication alignment
-  Enables BIMl readiness for trusted brand visibility in inboxes

Scales Across Teams and Regions

✦ Centralized management for multiple domains and environments

✦ Multi-tenant and white-label support for MSPs and MSSPs

✦ Role-based access for security, IT, and marketing teams

✦ API support for automation and integration

More Than DMARC

Hosted SPF, DKIM, DMARC, MTA-STS, and TLS-RPT

Visibility into transport-layer encryption gaps

Continuous monitoring to prevent configuration drift

Proven and Trusted



Rated **4.9/5** on **G2** for ease of use

Trusted by enterprises, governments, and service providers worldwide

Take the Next Step With PowerDMARC

Get Started

1

Protect client domains from impersonation



2

Identify spoofing sources



3

Enforce DMARC at your own pace

Secure your email identity with PowerDMARC.