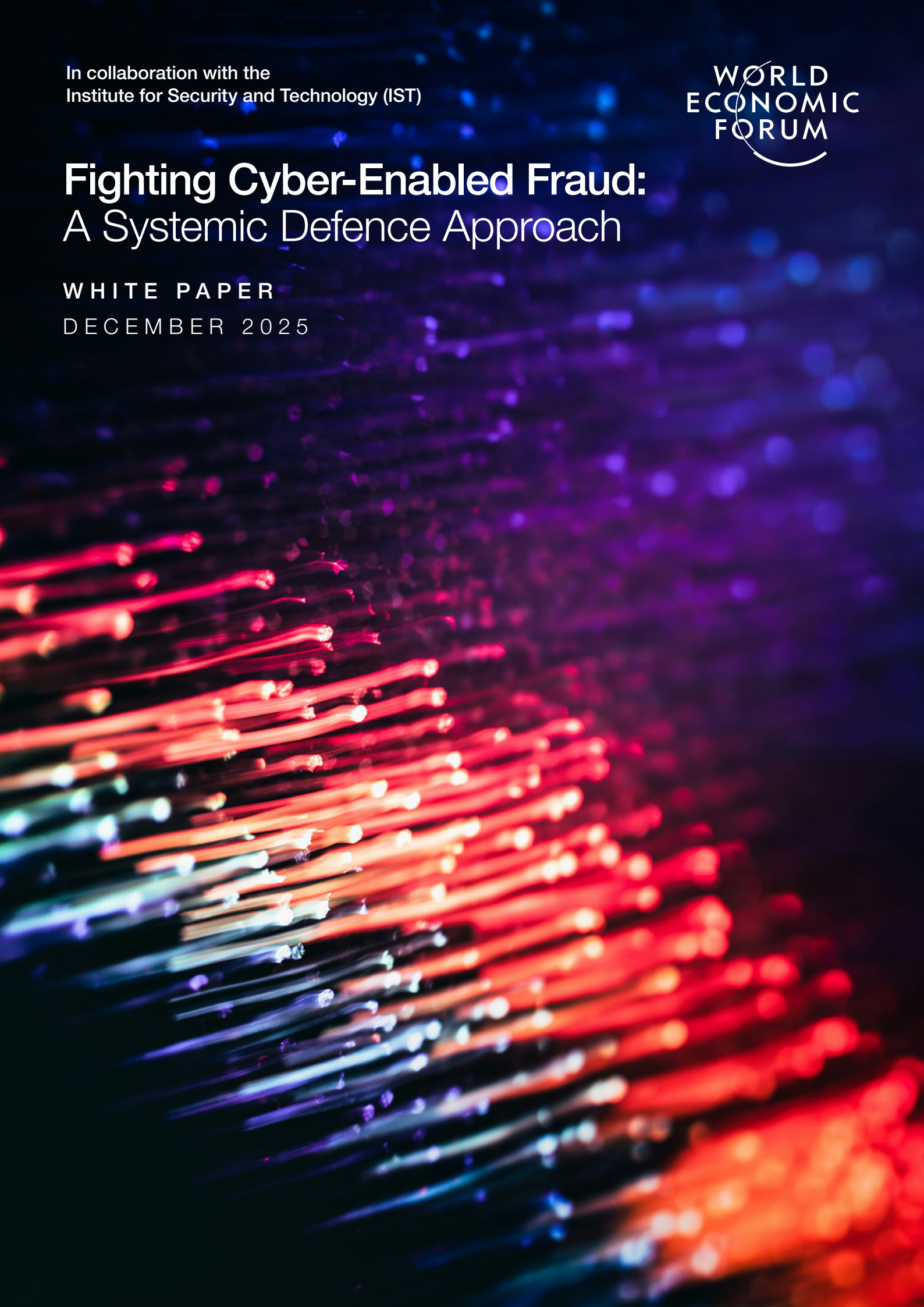
In collaboration with the
Institute for Security and Technology (IST)

WORLD ECONOMIC FORUM

# Fighting Cyber-Enabled Fraud:
## A Systemic Defence Approach

**WHITE PAPER**

DECEMBER 2025



**Images:** Unsplash +

# Contents

# Foreword

**Philip Reiner**
Chief Executive Officer and Co-Founder, Institute for Security and Technology (IST)

**Akshay Joshi**
Head, Centre for Cybersecurity; Member of the Executive Committee, World Economic Forum

Three decades after the internet became publicly available, digital connectivity has become as vital to societies as physical infrastructure – enabling economic growth, social inclusion and innovation on a global scale. Originally designed to foster openness and collaboration among researchers, the internet's architecture was not built with the safeguards needed for today's scale and complexity. This gap has created a digital environment that, while enabling unprecedented opportunity and growth, also exposes individuals and organizations to increasingly sophisticated threats such as frauds and scams – underscoring the need for systemic resilience and collective action.

Recognizing the need to rebalance responsibility for cybersecurity, the World Economic Forum's Partnership against Cybercrime – together with the Institute for Security and Technology (IST) – led the *Advancing Systemic Defence* working group to fight phishing and cyber-enabled fraud. Building on the Partnership's progress in fostering public–private operational collaboration, this effort seeks to advance shared responsibility throughout the digital ecosystem by stimulating coordinated action and required policy reforms by the key stakeholders.

There is no single blueprint for addressing such a complex challenge, but there is growing global consensus on the urgency to act. This white paper contributes to that effort by presenting key insights and outlining targeted opportunities for systemic solutions. Its aim is not to attribute fault, but to translate this shared urgency into coordinated action – mobilizing governments, industry leaders and civil society to strengthen the collective capacity to prevent, protect against and mitigate cyber-enabled fraud across the digital ecosystem.

Those who build and operate digital infrastructure share a responsibility to protect the public good. Just like the physical foundations of modern life, digital infrastructure must be designed and maintained to serve society safely and sustainably. Meeting this challenge requires collective, forward-leaning action to complement existing approaches aimed at strengthening the digital environment to prevent abuse and protect the people and communities who rely on it every day. This white paper serves as a call to action: now is the time to join forces across sectors and borders to build a digital ecosystem that is secure by design and resilient by default.

# Executive summary

## The accelerating scale and impact of phishing and cyber-enabled fraud call for systemic action.

**Phishing** and **cyber-enabled fraud** are a growing global threat to users, consumers, organizations and countries. The World Economic Forum's Partnership against Cybercrime, in collaboration with the Institute for Security and Technology (IST), developed a systemic defence framework to address this issue.

This approach explores how a multistakeholder model can shift responsibility upstream, empowering those best positioned to act at scale and prevent harm from taking root in the first place. These efforts sit in the space between public awareness initiatives – which aim to educate users about online risks – and law enforcement disruption campaigns that target criminal networks once harm has occurred.

This paper calls on stakeholders to act across three complementary pillars of systemic defence:

1. **Prevention:** Structurally reducing abuse before it occurs

   Prevention focuses on embedding safeguards at the foundational layers of the internet to reduce bad actors' ability to acquire, build or operate digital infrastructure for malicious purposes. Actions include strengthening risk-based due diligence and oversight in domain registration and hosting to detect and prevent misuse long before harm occurs.

2. **Protection:** Embedding user safety by default

   Protection calls for proactive, scalable solutions for consumer-facing services – such as email, browsers and messaging platforms – to shield users from phishing and cyber-enabled fraud. Governments can accelerate adoption and impact through national coordination hubs, enabling regulation and targeted incentives that raise the baseline of digital safety.

3. **Mitigation:** Enabling rapid, collective response

   Even with prevention and protection in place, timely detection and response remain essential. This paper calls for ecosystem-wide signal sharing – the exchange of verified, privacy-preserving indicators of abuse – and for incentives that promote effective action by relevant stakeholders. AI-assisted threat detection can enhance collaboration and enable response at the speed and scale required to contain sophisticated criminal infrastructures.

The actions proposed in this paper build on proven approaches already taking shape at the national level, while charting new pathways for collaboration and scale. By taking advantage of this momentum, it will be possible to strengthen systemic defence and foster a cohesive community of stakeholders committed to reducing the growing threat of phishing and cyber-enabled fraud.

Technical terms in **blue bold** are explained in the Glossary (see Appendix).

# Introduction

## The growing scale and impact of cyber-enabled fraud and phishing are escalating to become one of today's most pressing global challenges.

Cyber-enabled fraud continues to increase in scale and exact a heavy toll on individuals and organizations around the world. Phishing – including **smishing**, **vishing** and other varieties – while hardly a novelty, remains at the core of these threats. Despite significant public- and private-sector efforts to pursue offenders, while also promoting security and educating potential victims, phishing persists as a significant vector for scams, fraud and cyber intrusion. As a result, several policy-makers (see Box 1) have begun calling for a shift in the cybersecurity burden of protecting consumers from scams and fraud, away from those with fewer resources who face the downstream effects towards those further upstream who are in the best position to act at scale. The goal of such shifts is to enable implementation of systemic solutions that operate at scale.

BOX 1 **National policy on shifting the burden**

> **Cyber risks for members of the public will be minimised by largely removing responsibilities for the security of digital products and services from small and medium-sized enterprises (SMEs) and individuals, and placing them with government, manufacturers and service suppliers.**
>
> *Netherlands Cybersecurity Strategy*,[1] p. 19

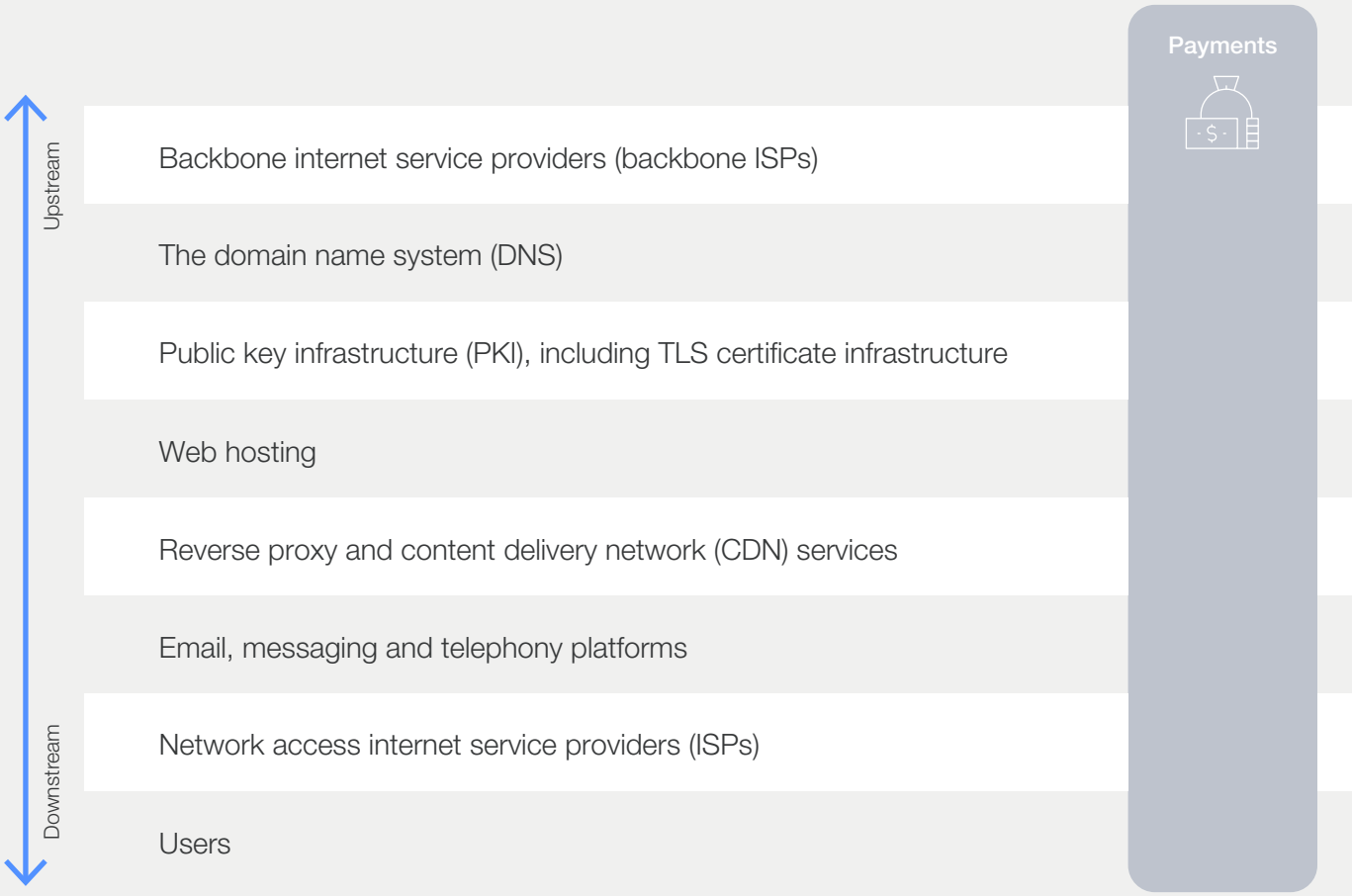
> **Today, end users bear too great a burden for mitigating cyber risks … The most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem.**
>
> *US National Cybersecurity Strategy*,[2] p. 4

> **This strategy aims to remove as much of the burden of cyber security from citizens as possible ... and transfer the burden of cyber security risk away from end users and towards those best placed to manage it.**
>
> *UK National Cyber Strategy*,[3] pp.36 and 66

The internet ecosystem is composed of layers of **digital infrastructure services** upon which consumer-facing online services rely, all underpinned by the payments ecosystem (see Figure 1). Understanding these layers in terms of upstream and downstream positioning reveals distinct opportunities for intervention:

- **Upstream digital infrastructure services** are those that supply foundational services upon which other companies and platforms build. These services include **backbone internet service providers (backbone ISPs)**, the **domain name system (DNS)**, **public key infrastructure (PKI)**, web hosting and **content delivery networks (CDNs)**. Because they often serve other businesses rather than end users directly, upstream providers may appear more distant from consumer harms; however, their actions to prevent fraud and abuse can have ecosystem-wide impact.
- **Downstream online consumer services** are those positioned closer to end users, and thus such providers face more direct user-trust risks than those upstream. These services include **"access" internet service providers (access ISPs)** and mobile network operators, consumer-facing platforms and application providers. Because they interact directly with end users, harms and abuses are more visible to them, often incentivizing bundled security services and robust trust and safety practices. These interventions have an immediate impact on served end users.

FIGURE 1 | **Depiction of the digital ecosystem***




* This white paper focuses primarily on upstream digital infrastructure services that underpin internet functionality and serve as high-leverage intervention points for countering phishing and cyber-enabled fraud. The analysis is not exhaustive and does not address every contributing factor or intervention opportunity (e.g. consumer-facing platforms that may serve as delivery mechanisms).

**Source:** World Economic Forum and IST

This paper is the culmination of a year-long study by the World Economic Forum and the Institute for Security and Technology (IST), supported by standing members of the Partnership against Cybercrime and informed by many other experts. Drawing on in-depth research, community meetings and workshops, together with expert consultations, this effort sits in the space between public awareness initiatives – which aim to educate users about online risks – and law enforcement disruption campaigns that target criminal networks once harm has occurred. It focuses on the systemic layer in between: the policies, standards and operational practices that can prevent abuse from taking root in the first place and enable more rapid detection of and response to in-progress abuse.

> **Cyber-enabled fraud erodes trust and targets the most vulnerable. To counter it, we must act together – governments, businesses and individuals – sharing intelligence, strengthening defences and making cyber resilience a national priority.**
>
> Sami Khoury, Government of Canada Senior Official for Cyber Security

# 1 State of the threat

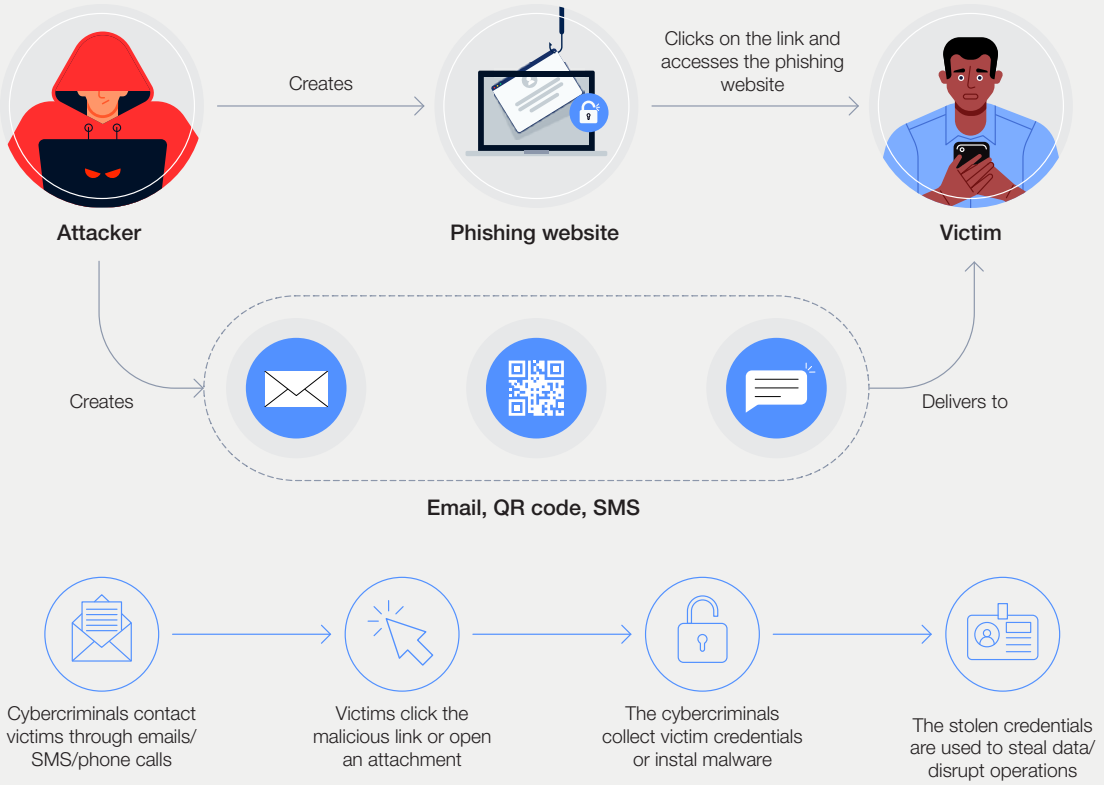
## Phishing and cyber-enabled fraud are growing at an alarming rate, fuelled by cybercriminals' use of AI.

From artificial intelligence (AI)-driven impersonation to transnational scam networks, cyber-enabled fraud has emerged as one of the most urgent and costly global threats, accounting for more than $1 trillion in losses in 2024.[4] These losses are more than staggering figures: they reflect a troubling evolution in cyber-enabled fraud spanning multiple dimensions of speed, scale and sophistication. At the same time, threat actors adapt quickly, iterating their tradecraft in direct response to defensive measures, and often operate across national borders – taking advantage of differences in legal systems, enforcement capacity, cyber-maturity levels and regulatory frameworks.[5]

Cyber-enabled fraud ranks as the second-highest organizational cyber risk after ransomware for 2025 according to respondents surveyed by the *Global Cybersecurity Outlook* report.[6] Phishing continues to serve as the backbone of cyber-enabled fraud, enabling crimes ranging from credential theft and ransomware to large-scale financial scams. Phishing messages now span email, short message service (SMS), messaging apps and social media – often directing victims to convincing fake websites built to steal credentials, capture financial data or deploy malware (see Figure 2).

According to the European Union (EU) Agency for Cybersecurity's report *Threat Landscape 2025*, phishing is the dominant intrusion vector, accounting for approximately 60% of cases.[7] Its growth shows no sign of slowing: credential-harvesting attacks surged sevenfold in the second half of 2024, while overall phishing threats doubled during the same period.[8] Advances in generative AI are making phishing both easier to conduct and more effective. Recent research highlights the scale of this shift: a 2024 study found that large language model (LLM)-generated phishing emails achieved click-through rates of 54%, matching human expert performance and outperforming an average phishing email by 350%.[9] The Anti-Phishing Working Group (APWG) reported the number of phishing attacks has continued to rise steadily, with an increase of 13% between the first and second quarter of this year.[10]

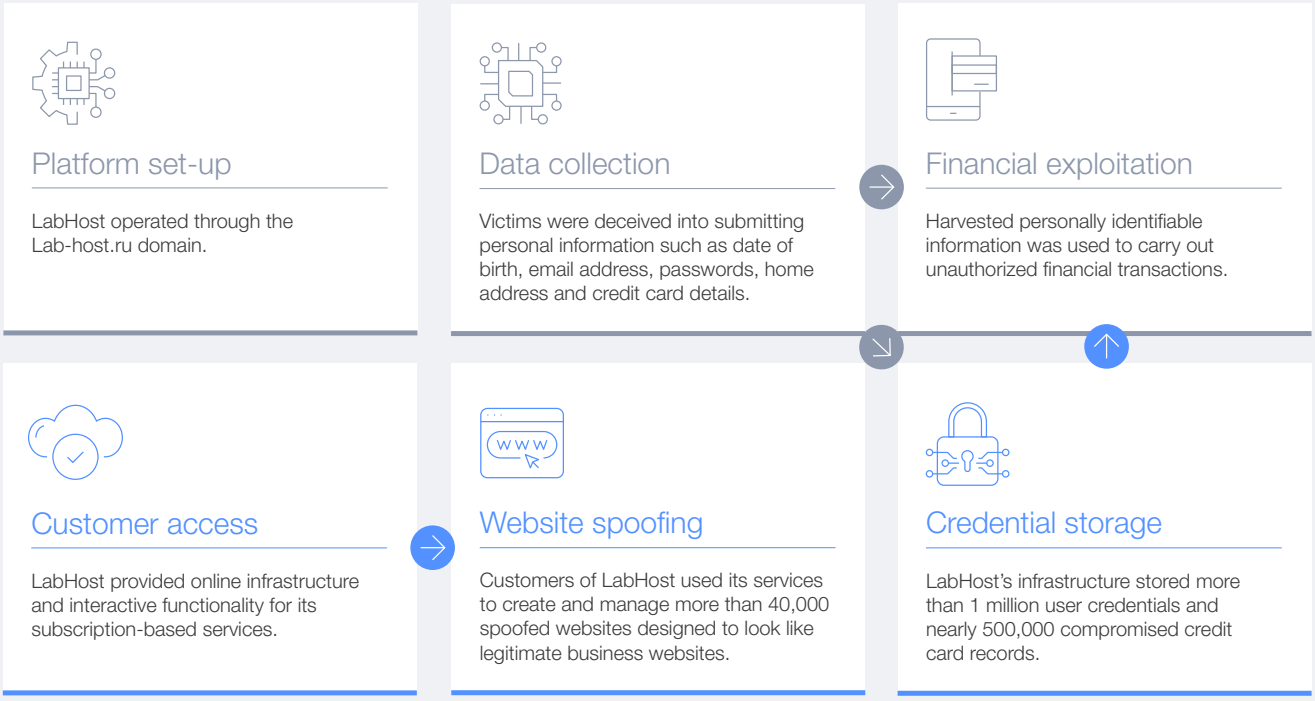
FIGURE 2 **Depiction of a phishing incident**




**Source:** Adapted from Cloudflare and TrendMicro

Phishing is often framed as a purely social engineering challenge, but its persistence and evolution are deeply tied to the digital infrastructure services that underpin the internet. Malicious actors exploit domain names, **transport layer security (TLS) certificates**, web-hosting platforms, **reverse proxies** and other digital infrastructure services to set up and scale phishing schemes, evade detection and increase their credibility with targets (see Box 2). This infrastructure – designed to support legitimate online activity – can be repurposed by threat actors for malicious purposes. Effective efforts to combat phishing require defenders to work collaboratively across the ecosystem, while implementing trust measures in ways that minimize inconvenience for legitimate users and preserve the internet's benefits.

BOX 2 **Phishing-as-a-service: Crime in a box**




Phishing-as-a-service (PhaaS) – a subset of the broader portfolio of crime-as-a-service (CaaS) offerings – has transformed phishing from a technique requiring technical skill into a commodity. Criminal groups sell ready-made phishing platforms, lowering the barrier of entry for less technically adroit actors and dramatically scaling the reach of attacks. Law enforcement has been actively disrupting PhaaS operations; some recent examples include:

**Realtime-Phishing:** A 2025 joint police operation led to the arrest of a university student in the UK who sold more than 1,000 phishing kits used to target banks and institutions worldwide, causing losses of at least £100 million globally.[11]

**16shop:** An International Criminal Police Organization (INTERPOL)-led operation in 2023 shut down this phishing platform, leading to arrests in Indonesia and Japan. 16shop sold phishing kits that enabled attacks against more than 70,000 victims in 43 countries.[12]

**LabHost:** A European Union Agency for Law Enforcement Cooperation (Europol)-coordinated action in 2024 involving 19 countries dismantled this platform, arresting 37 suspects.[13] With 10,000 users and links to 40,000 phishing domains, LabHost offered subscription-based services such as phishing kits, hosting and LabRat, a tool for stealing credentials and bypassing two-factor authentication.[14]

**Operation First Light 2024:** A global police operation spanning 61 countries targeted phishing, fraud and impersonation scams. It resulted in 3,950 arrests, the identification of more than 14,600 suspects and the seizure of $257 million in assets, including cash, cryptocurrency, real estate and luxury goods.[15]

> **Phishing, as part of the broader category of online scams, tops the list of cybercrimes INTERPOL's membership is tackling now, both by volume and economic impact. INTERPOL is actively working with partners worldwide to help law enforcement combat transnational cybercrime more effectively – and calls on all stakeholders to join these efforts.**
>
> Neal Jetton, Cybercrime Director, INTERPOL

## 1.1 Criminals exploit digital infrastructure services at scale

Phishing campaigns depend on a set of legitimate infrastructure services that have been repurposed for abuse. As discussed in more detail below, these include domain names (influenced by automation and low pricing), subdomains, reverse proxy services and delivery mechanisms.

**Malicious domain registration remains a persistent, large-scale problem:** In 2024, cyber criminals used more than 8.6 million unique domain names in cyberattacks – an 81% increase over the previous year.[16] The NetBeacon Institute recently observed "the largest month-on-month increase in unique domain names associated with phishing (63%). Most (87%) of this phishing was classified as 'maliciously registered'. The bulk of this malicious phishing was concentrated among a few registrars […]."[17] An Internet Corporation for Assigned Names and Numbers (ICANN)-funded study similarly found that a mere 20 registrars, out of the more than 3,000 accredited, accounted for nearly 84% of maliciously registered domains found within a sample set.[18] ICANN further observed that "discounted pricing and bulk registration opportunities were strongly associated with abuse".[19] While it did not define a fixed numerical or time-based threshold for "bulk" registration, the study examined bulk-related features such as bulk discounts, free bulk search and prerequisite-free application programming interface (API) access as associated indicators.

**Services are a growing enabler of phishing:** Subdomains (e.g. *mail*.example.com) – commonly offered through hosting providers, website builders and software-as-a-service (SaaS) platforms – are increasingly being exploited for phishing. Between roughly one-quarter (24%)[20] and one-third (36.27%)[21] of phishing attacks in recent years made use of subdomains, more than doubling between 2021 and 2024.[22] Additionally, Interisle's most recent phishing landscape report observed that "89% of the subdomain-provider attacks occurred on domains operated by just ten providers, which shows how the choices made by a few companies can affect the phishing landscape".[23] Any measures taken to prevent abuse are voluntary, unless required under the upstream registrar's own terms of service or mandated by local regulations. When subdomain providers fail to act, registrars may be pressed to suspend the parent domain – but such steps carry the risk of extensive collateral damage, disabling hundreds or thousands of legitimate services at once.[24]

**Automation in domain registration and configuration fuels the speed and scale of abuse:** Bad actors leverage automation to create multiple accounts and register domains at speed and scale. The availability of unrestricted APIs enables large-scale, automated domain creation and configuration, which attackers use to rapidly deploy phishing infrastructure.[25] ICANN found that registrars permitting API access saw a fourfold increase in malicious activity,[26] and according to the NetBeacon Institute, introducing friction to slow abuse at scale, such as requiring new registrants to pass a basic trust threshold at the registrar before gaining access to programmatic registration tools, could be part of the solution.[27]

**Domain hijacking through account takeover drives online fraud:** Domain hijacking through account takeover is a major driver of online fraud, as attackers gain unauthorized access to domain registrant accounts – often using stolen or reused credentials – to seize control of valuable domains.[28] Once hijacked, these domains can be exploited for malicious purposes such as phishing campaigns, spreading malware, impersonating legitimate brands or redirecting users to fraudulent websites. Strengthening authentication, monitoring suspicious activity and enforcing strict access controls are key to preventing such fraudulent takeover.

**Reverse proxy services can shield and legitimize phishing infrastructure:** Reverse proxy services serve legitimate purposes – improving performance, providing protections against distributed denial of service (DDoS) attacks and enhancing security for websites worldwide. However, they also offer concealment advantages that criminals have been observed exploiting.[29,30,31] By terminating encrypted TLS sessions at the proxy endpoint, they mask the true hosting origin of malicious websites, re-encrypt traffic and present only the proxy's reputable infrastructure to victims and investigators. This provides anonymity, free TLS certificates (which enables the trusted padlock icon to appear in the user's browser), high performance and resilience – key enablers for phishing. Many providers bundle reverse proxy, content delivery network (CDN) and security services, but it is the proxy function that most directly facilitates abuse.

BOX 3 | **Funnull: A criminal proxy service**

In 2025, the United States Federal Bureau of Investigation (FBI) issued a cybersecurity advisory on Funnull, a criminally operated infrastructure service supporting large-scale cryptocurrency fraud and phishing campaigns.[32] At the same time, the US Treasury's Office of Foreign Assets Control (OFAC) announced sanctions on Funnull and its administrator for enabling hundreds of thousands of fraudulent sites involved in virtual currency investment scams by purchasing internet protocol (IP) addresses and registering hundreds of thousands of domains in bulk from major cloud service companies worldwide and selling them to cybercriminals to host scam platforms and other malicious web content.[33,34]

The case illustrates how illicit infrastructure can be purpose-built for abuse, mirroring the techniques available through legitimate services but dedicated entirely to criminal activity. Funnull's takedown highlights the importance of targeting malicious infrastructure providers while also strengthening cooperation with legitimate intermediaries to prevent abuse.

**Text messaging and voice calls are a prominent and growing phishing vector:** While email remains the primary phishing delivery mechanism, text messaging (smishing) and voice calls (vishing) have emerged as prominent and rapidly growing attack vectors. Fraudsters exploit SIM farms – devices that emulate large banks of cell phones – and "Cash for SMS" apps that rent unused messages to bypass legitimate channels and send scam messages at scale. The volume is immense: UK operators have blocked more than 1 billion suspected scam texts since 2023, while voice phishing attacks surged by 442% in 2024, driven by AI-powered social engineering.[35,36] These attacks have affected 70% of organizations globally.[37] Migration to internet-based protocols such as rich communication services (RCS) offers security improvements over traditional SMS, including verified sender identities and encryption in transit. However, implementation gaps have introduced new vulnerabilities. Attackers exploit inconsistent verification systems to spoof verified brands and bypass traditional SMS filters, taking advantage of the convergence of mobile and internet messaging to evade carrier-level controls.[38] Regulatory approaches to smishing remain under development, with effective solutions, such as SMS inspection, needing to be reconciled with privacy requirements.[39]

> **Cyber-enabled fraud is one of the most pressing threats facing the digital economy today. At Mastercard, we believe that a systemic defence approach – anchored in collaboration, threat intelligence and proactive controls – is essential to protecting consumers and businesses alike. As we work across the digital ecosystem to strengthen prevention, embed security-by-design and accelerate mitigation, we can raise the collective resilience of the digital infrastructure we all rely on.**
>
> Johan Gerber, Global Head of Security Solutions, Mastercard

# 2 A systemic defence approach

## Turning the tide on cyber-enabled fraud requires a systemic approach incorporating prevention, protection and mitigation.

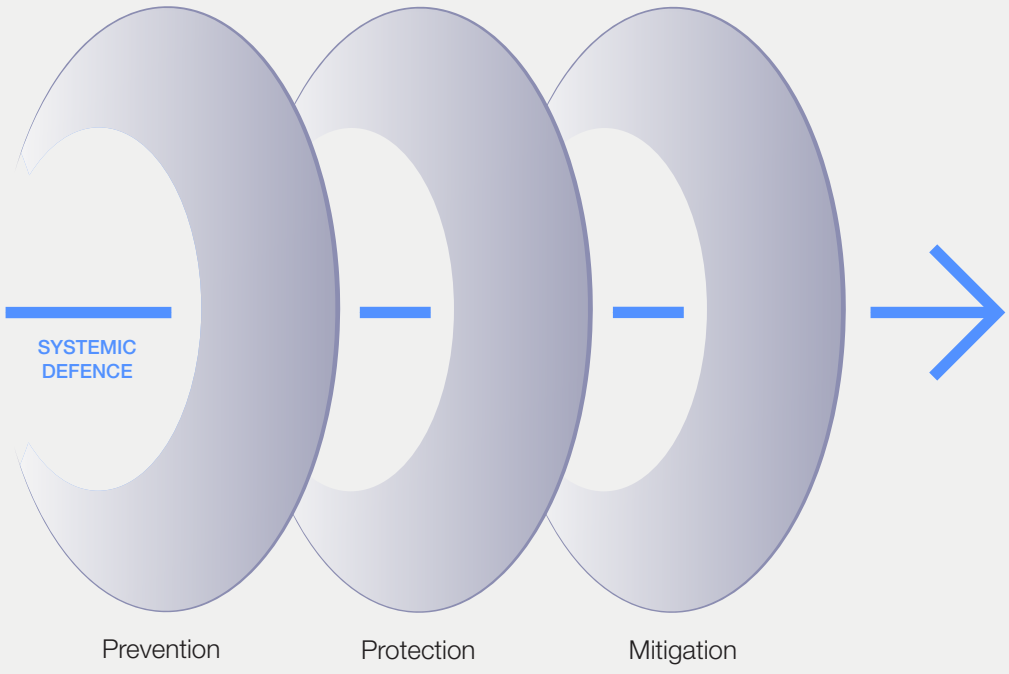
The Partnership against Cybercrime developed a set of "systemic defence" actions to fight phishing and cyber-enabled fraud. These actions – taking in prevention, protection and mitigation – emerged from an examination of the opportunity space represented by the mapping of the global digital ecosystem's layers depicted earlier in Figure 1.

Effective systemic defence requires a balanced model that maximizes the leverage of upstream interventions while ensuring broad, reliable coverage through downstream measures.[40]

Drawing from the research and expert consultations, the community derived a strategic systemic defence framework, structured around tangible actions to affect phishing and cyber-enabled crime (see Figure 3). It involves three components, each mutually reinforcing:

- **Preventive** actions focus on structurally reducing bad actors' ability to acquire, build or operationalize digital infrastructure at the upstream level.
- **Protective** actions focus on building systemic safeguards within downstream services. These measures reduce harm by alerting, shielding and empowering users against fraud, phishing and other forms of cyber-enabled abuse.
- **Mitigation** actions focus on improving the ecosystem-wide capability to identify abuse, enable effective reporting and share actionable signals, while also supporting rapid responses to take down malicious activities from upstream infrastructure and update downstream protection efforts.

FIGURE 3 **Systemic defence framework**




**Source:** World Economic Forum and IST

## 2.1 Prevention

The internet's decentralized, multistakeholder governance model – a deliberate design choice – has fostered resilience, innovation and global participation for decades. This distributed architecture enables open access, flexibility and a diversity of voices shaping how the internet evolves.

At the "names and numbers" layer, where the fundamental addressing and routing functions of the internet reside, governance is distributed among multiple entities. The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates global policy for generic top-level domains (gTLDs) such as ".com" or ".org" through a multistakeholder process, while country-code top-level domain (ccTLD) operators manage their namespaces such as ".uk" or ".in" under varied governance models – from independent multistakeholder foundations to direct governmental or commercial oversight. This distributed governance model correlates to a divergent cybercrime landscape. On average, the abuse rates for ccTLDs are statistically significantly lower than for gTLDs.[41]

### BOX 4 ICANN's role in ensuring a stable, secure and unified global internet

ICANN has progressively strengthened requirements in its contracts with generic top-level domain (gTLD) registry operators and registrars. These obligations, set forth in the Registrar Accreditation Agreement (RAA), the Registry Agreements (RAs) and the ICANN policies incorporated into them, include a wide range of requirements designed to preserve the security, stability and resilience of the DNS.

Since 2013, the RAA has required registrars to maintain public abuse contacts, publish a description of their abuse procedures and reasonably investigate and respond to reports of **DNS abuse**. The RAs have required registries to publish abuse contact information and perform technical analyses to determine whether their sponsored domain names are being used to perpetrate DNS abuse. Additional requirements such as those related to the accuracy and accessibility of registration data and taking action to remove orphan glue records[42] associated with malicious activity are also present in the agreements enforced by ICANN.

In 2024, amendments introduced further enhancements: they defined DNS abuse for the purposes of the RA and RAA, required simple abuse reporting channels with timely acknowledgement and obligated providers to take mitigation actions promptly once presented with credible evidence.[43,44] ICANN's Contractual Compliance function monitors and vigorously enforces these contractual requirements.

As part of its wider DNS Abuse Mitigation Program, ICANN also provides capacity development and training to community members engaged in combating DNS abuse. New transparency tools, such as the Domain Metrica platform, provide public visibility into abuse patterns across the DNS, while the Inferential Analysis of Maliciously Registered Domains (INFERMAL) project aimed to better understand attackers' preferences regarding DNS abuse.[45,46]

Looking ahead, ICANN and its stakeholders are discussing additional preventive measures. Ideas under consideration include requiring registrars to review associated domains once abuse is confirmed in one of them and adding safeguards to introduce friction to the registration process prior to domain activation, particularly for bulk domain purchases by new customers.[47,48]

This decentralized ecosystem of responsibility ensures stability and resilience; however, malicious actors exploit gaps among jurisdictions, governance models and enforcement capacities – rapidly registering domains, spinning up infrastructure and using trusted intermediaries to operationalize fraud and scams at scale. Abuse reporting and timely response actions are essential to curb in-progress harms, but reactive measures alone still leave ample opportunity for malicious actors to cause damage, making the case for due attention to *preventive* measures. Some within the industry refer to these as "anti-fraud" measures.[49] For example, ICANN research found that "stringent registrar restrictions" are associated with a 63% decrease in the number of maliciously registered domains, and validation of registrant information during account creation or before domain purchase is associated with a 70% drop.[50]


> **The Global Cyber Alliance takes a systemic approach to fostering collective action among internet infrastructure operators. Building on the global success of MANRS for routing security, our data-driven and community-based model powers initiatives like Domain Trust and AIDE – uniting registries, registrars, hosting providers and network operators to tackle abuse and measure real-world impact.**
>
> Leslie Daigle, Chief Technical Officer and Internet Integrity Program Director, Global Cyber Alliance

Beyond the names and numbers layer, multiple infrastructure domains offer structural opportunities for upstream prevention. Telecommunications infrastructure – including mobile networks, SMS routing systems and voice services – can implement authentication and verification measures that raise the barriers to abuse. These require a close support and alignment of national authorities to enforce the homogeneous application of such measures across the ecosystem. Cloud and hosting services – including reverse proxies, content delivery networks and managed hosting – have the capability to embed abuse detection and verification mechanisms into their service offerings. Payment systems and financial intermediaries can apply risk-based controls that disrupt fraud monetization pathways, while identity and authentication services can strengthen verification processes that make impersonation more difficult. Each of these layers represents an opportunity for service providers, platforms and intermediaries to implement upstream safeguards that structurally reduce the operational capacity available to bad actors, often while improving service quality and trust for legitimate users.

While the results will no doubt vary across digital infrastructure services and individual providers, the evidence points to meaningful opportunity: preventive controls reduce criminals' ability to acquire and operationalize digital infrastructure to further their schemes.

## A call for industry stakeholders to strengthen preventive controls

Preventive actions must focus on structurally reducing bad actors' ability to acquire, build or operationalize upstream digital infrastructure. Rather than relying solely on reactive takedowns or end-user vigilance, prevention seeks to embed systemic safeguards at the foundational layers of the internet – where abuse begins. By reinforcing integrity and accountability in domain registration, hosting, telecommunications and identity provisioning, prevention measures can shrink the surface area available for cyber-enabled crime and protect citizens long before harm occurs.

**Action 1 – Strengthen risk-based customer due diligence practices in digital infrastructure services:** Based on the above, upstream digital infrastructure service providers should be required to implement risk-based customer due diligence practices.[51] For standard and lower-risk services, validation should at the very least include syntactical error checking and verification that key attributes (e.g. name, organization, contact information, country) are consistent, complete and demonstrably linked to a real, reachable entity.[52] Such a practice would be consistent with requirements outlined in the EU's Network and Information Systems Directive 2 (NIS2).[53] For higher-risk services – such as bulk domain registration and bulk messaging services – providers should require the use of traceable

instruments connected to the account holder (e.g. financial/payment traceability). This practice would leverage trust frameworks long in use such as those within the financial services sector. Where available, governmental digital identity programmes – such as those in Belgium, Estonia and several US states and provided for by upcoming EU initiatives (e.g. the Regulation on Electronic Identification and Trust Services [eIDAS])[54] – should be used to strengthen verification processes and reduce fraud risk.

**Action 2 – Tighten oversight of bulk domain registrations and subdomain services:** To reduce the prevalence of malicious bulk domain registrations in phishing and cyber-enabled fraud activities, registrars should restrict high-volume registration activities to established business customers with low-risk profiles. Building on customer due diligence practices, organizational identity should be robustly verified, payment methods attributed and customers should demonstrate positive track records over time. Volume and time-based thresholds for what constitutes "bulk registration" should be established through transparent, multistakeholder policy processes. For any provider that generates subdomains for third parties, the upstream registrar should require minimum abuse-prevention practices including account verification, monitoring high-volume subdomain creation and participation in signal-sharing collaboratives. Preventive measures should focus on detecting malicious subdomains at enrolment or early in their life cycle, while avoiding blunt interventions (such as suspending entire domains) that risk collateral damage to legitimate services. ICANN, ccTLD managers and national governments should explore mechanisms to embed such requirements into registry and registrar obligations, ensuring that they flow downstream to subdomain providers.

**Action 3 – Explore a short public notice period before new domains go live:** Phishing domains are often delegated to the DNS and weaponized within hours of registration, giving defenders very little opportunity to act before abuse begins. One potential safeguard is to require all new domains to be publicly listed upon registration but withheld from delegation for a short, fixed time period (e.g. 24–48 hours). Many legitimate registrants do not place new domains into immediate use, registering them for future needs, so such a delay would not burden most users. It would, however, create a window for pre-activation detection of abusive or deceptive domains. Some registrants may have legitimate needs for immediate delegation, so mechanisms such as a refundable deposit – combined with accurate registrant information and a trusted payment source – could provide a fast-track option while maintaining safeguards. Bad actors could attempt to use the fast-track option, but the added cost and administrative burden might not align with their business model. Other registrants might not wish to have their domain publicly listed before delegation for intellectual property-related, competitiveness or privacy reasons. In those cases, conditional exceptions as mentioned above should be introduced.

> **Cybercrime is a global challenge that exploits legitimate infrastructure and undermines trust in our interconnected systems. Through the work of the Partnership against Cybercrime, and tools like NetBeacon Reporter, we can collaborate widely across industries, including cybersecurity specialists, governments, law enforcement and individuals, to scale the disruption of threats like phishing and malware, making the internet safer for all.**
>
> Graeme Bunton, Executive Director, NetBeacon

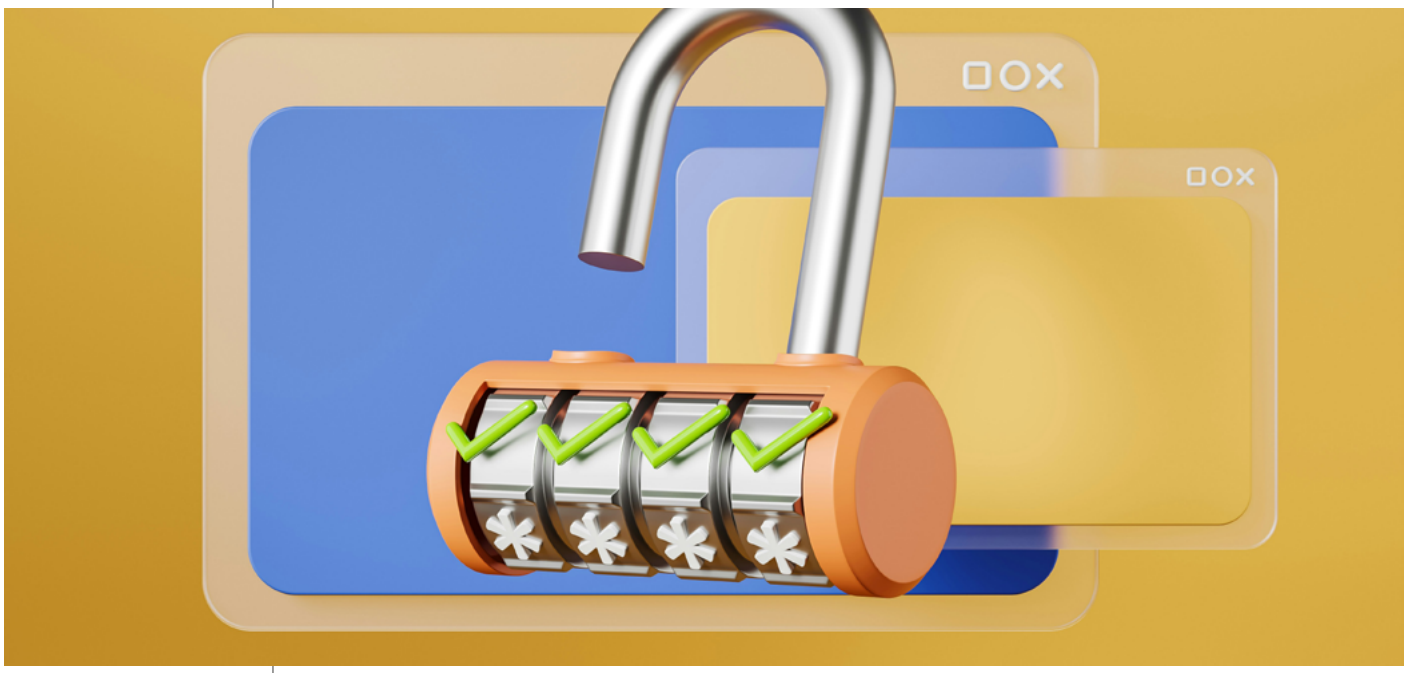
## 2.2 Protection

Protective actions focus on building systemic safeguards within downstream services that alert, shield and empower users against fraud and phishing. The objective is to reduce harm by ensuring that individuals, organizations and communities benefit from proactive defences embedded across the digital ecosystem.

Internet service providers, technology companies and infrastructure operators can play a critical role by blocking known malicious activity and ensuring that security features are available by default. Protective DNS systems – like that offered by non-profit Quad9 – block access to known malicious domains at the resolution level, while email authentication protocols such as DMARC prevent email spoofing when properly implemented. Despite their promise, these measures suffer from inconsistent implementation, user resistance to added inconvenience, and attackers' rapid adaptation, limiting their effectiveness against the speed and scale of modern phishing campaigns.

National governments play a unique role in strengthening digital safety through their regulatory authority, convening power and ability to reshape market dynamics. In several jurisdictions, dedicated anti-scam centres serve as national coordination hubs, uniting agencies, law enforcement and the private sector. Beyond enforcement, governments can encourage stronger practices by supporting voluntary alliances, incentivizing innovation and providing positive recognition for stakeholders that improve defences.[55] Without coordinated enforcement by national authorities and consistent implementation by stakeholders, uneven application of measures could leave gaps exploitable by malicious actors.

Yet government action remains uneven across jurisdictions, with insufficient mutual learning and many governments lacking development efforts. Some governments lack the institutional capacity to coordinate frameworks or engage in cross-border collaboration, while others struggle to incentivize providers to take action. These gaps are particularly acute in developing countries, where limited institutional capacities, varying levels of digital adoption, informal marketplaces and entrenched criminal networks create fertile ground for cyber-enabled fraud. The newly adopted United Nations Convention against Cybercrime could become a reference point for new state-level policies in this realm.[56]



> **At Quad9, our mission is to provide a safer and more robust Internet for everyone. As a Swiss non-profit, we offer free, privacy-focused DNS security services that block malware, phishing and spyware – protecting over 100 million users every day. With more than 245 locations in 115+ countries, we're working to enhance privacy, reduce cyber harm in vulnerable regions, and improve internet performance in underserved areas.**
>
> Simon Forster, General Manager, Quad9

BOX 5 | **National models for cyber defence**

A number of governments have implemented notable approaches to counter phishing and cyber-enabled fraud, illustrating different pathways for capacity-building, regulation and citizen engagement. While the models below have been established chiefly to deal with cybersecurity – with fraud and scams only sometimes featuring as an element of the model – some governments have gone further by establishing a dedicated coordinating body set up to focus efforts and expertise on fraud and scams.

**Australia** implements a whole-of-nation strategy emphasizing shared responsibility, which has been embodied by the creation of a multidisciplinary National Anti-Scam Centre bringing together competences from across the various government agencies dealing with fraud and scams. Its Scams Prevention Framework, which is due to come into force in 2026, imposes enforceable requirements on telecom, financial and platform providers, with penalties for non-compliance.

**Canada**'s Centre for Cyber Security (CSE) and the Canadian Internet Registration Authority partnered to launch Canadian Shield in April 2020: a free DNS-firewall service that blocks access to malicious domains flagged for phishing, malware or scam activities. By routing users through trusted DNS resolvers, it prevents fraud efforts before they reach the end device. Over the past 12 months, Canadian Shield was used by 2.81 million users, who benefited from around 800 million DNS blocks, resulting in a reduction of visits to malware, phishing and botnet sites.

**India**'s CERT-In, through an AI and situational awareness system, analysed more than 9,800 billion DNS queries in the course of 2024, detecting 2.2 billion queries linked to malicious domains, of which 128 million were phishing-related. A total of 3,044 phishing sites were mitigated, affecting nearly 695,000 users. CERT-In also regularly shares DNS-based threat intelligence with global partners to strengthen international cooperation and secure the digital ecosystem.

**Singapore** adopts a whole-of-nation strategy to counter malicious online activity. The Singapore Police Force (SPF) collaborates with other government agencies, such as the Cyber Security Agency of Singapore (CSA) and the Infocomm Media Development Authority (IMDA), and the private sector to disrupt scam enablers (such as fraudulent communication and marketing channels). International collaboration is also a key pillar in enabling the SPF to take down transnational scam syndicates. These efforts are underpinned by public education campaigns aimed at cultivating digital scepticism to develop a more scam-savvy populace.

**Switzerland** strengthens domain-level defences through proactive disruption. The 2015 Ordinance on Internet Domains (OID) empowers the national domain registry and cybercrime-recognized organizations to act swiftly against online abuse. When domains under ".ch" or ".swiss" are suspected of hosting phishing, malware distribution or botnet activity, they can be blocked or sinkholed for up to 30 days, disrupting malicious infrastructure and reducing potential harm.

**The United Kingdom** has developed the Online Safety Act, which requires social media platforms and search engines to protect their users from fraudulent content and, for larger organizations, from fraudulent advertising. This is part of a broader national effort supported by strong public–private partnerships through an Online Fraud Charter signed by some of the biggest global tech companies and a recently updated Telecommunications Charter. Underpinning this national response, the Fraud Strategy establishes a coordinated framework built on new legislation, improved enforcement mechanisms, increased industry cooperation and public–private data-sharing to proactively identify and prevent fraud.

## A call to accelerate user protections by default

Embedding protective tools as defaults creates a more resilient ecosystem, ensuring that security reaches citizens directly and equitably. Targeted interventions can substantially reduce phishing success by hardening the interfaces where users make trust decisions: web browsers, messaging apps, voice calls and authentication methods. Each addresses a distinct attack vector while reinforcing broader protective infrastructure.

**Action 4 – Bring transparency to website trust and block known threats by default:** Users struggle to distinguish legitimate websites from fraudulent sites because a browser's lock icon signals an encrypted connection but not who is at the other end of it. Belgium's Safeonweb browser extension demonstrates a user-facing solution: colour-coded trust signals based on the website owner's level of verification and threat intelligence (see Box 6). Extended validation certificates attempted similar goals but failed after browsers removed prominent indicators around 2019.[57] Given skyrocketing phishing and fraud levels, users need clear trust signals more than ever. A modernized approach requires standardized, prominent browser indicators distinguishing verified organizations from anonymous sites, leveraging governmental digital identity frameworks such as eIDAS where available alongside industry-led alternatives. Complementing browser-level signals,

infrastructure operators should deploy back-end protective measures preventing users from reaching malicious sites entirely. Internet service providers and network operators should offer protective DNS as default, drawing from shared threat intelligence feeds updated in real time. Browsers and security software should implement block-listing mechanisms that prevent access to known malicious domains. Success requires coordinated action among certificate authorities, browser vendors, DNS providers and regulators.

BOX 6 **Belgium's Safeonweb: A model for browser trust signals**

Centre for Cybersecurity Belgium developed the Safeonweb browser[58] extension to help citizens assess website trustworthiness through simple visual indicators. The extension displays colour-coded signals for every website visited: green indicates that the owner has been validated, orange shows that the owner cannot be verified and red warns that the site is known to be malicious or insecure.

Organizations with a Belgian Enterprise Number can register their domains for free on the Safeonweb@Work platform. The system integrates real-time threat intelligence – if a validated site is compromised, its status immediately changes to orange or red. The extension analyses the certificate validation level, the certificate authority that issued it and whether the domain is registered as malicious. With more than 50,000 users, the extension demonstrates how government-led initiatives can combine organizational verification with active threat monitoring. The programme's success suggests that similar national or regional initiatives could scale globally with proper coordination and interoperability standards.

**Action 5 – Strengthen user protections against messaging and voice phishing:** Telecommunications providers and messaging platforms should strengthen safeguards that alert and empower users against text and voice phishing. For verified business communications, they should establish mandatory sender verification standards across RCS implementations that use existing trust infrastructures – such as Certificate Authority Extended Validation and governmental digital identity programmes (e.g. eIDAS) – displaying prominent visual indicators including logos and verified checkmarks. As called out by Europol in its new position paper on caller ID spoofing, international coordination on interoperable technical standards is essential for cross-border effectiveness.[59] Building on existing mobile network industry baseline controls for preventing unsolicited messaging traffic,[60] for unknown senders, devices should display default warnings with blocking and reporting options, flagging patterns associated with phishing such as fake delivery notifications or suspicious links. Organizations should deploy AI-powered detection systems to identify emerging fraud campaigns and provide contextual risk warnings to users. Voice protection measures can be enhanced by combining caller authentication with real-time fraud scoring, helping to flag suspicious activity as it happens. These security efforts should be carefully balanced with usability, ensuring that protections remain accessible and supported by clear user education.

**Action 6 – Accelerate phishing-resistant authentication and harden legacy methods:** Traditional multifactor authentication (MFA) has improved account security and reduced fraud and account takeover but attackers increasingly bypass it. Phishing-resistant solutions such as passkeys offer far greater protection and meet US National Institute of Standards and Technology (NIST) and European Union Agency for Cybersecurity (ENISA) high assurance standards. Yet most regulations still mandate outdated MFA technologies. Governments should design regulations driving adoption of phishing-resistant authentication, rewarding providers who implement state-of-the-art safeguards. Meanwhile, legacy methods such as SMS one-time passwords will persist, particularly in emerging markets and must be systematically hardened.[61] Telecommunications providers should strengthen validation standards, secure delivery channels and enforce sender ID registries to block spoofing.[62] Regulators must reinforce these with mandatory anti-spoofing controls and oversight. Achieving this in practice necessitates an evaluation of the associated costs and benefits. Until phishing-resistant methods achieve universal adoption, coordinated action by telecommunication providers, online platforms and regulators is essential to ensure that legacy mechanisms deliver the strongest possible protection.

# 2.3 Mitigation

When prevention and protection measures fail and digital infrastructure is abused, rapid detection and coordinated response become critical. Effective defence requires coordination among hundreds of organizations generating threat intelligence and hundreds more positioned to act – from security vendors and financial institutions to domain registrars and hosting providers. Yet no single organization can maintain bilateral relationships at the required speed and scale, creating a many-to-many coordination problem.

Diverse networks have emerged to address this challenge. Industry-specific platforms such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and NetBeacon Reporter[63] for domain names standardize abuse reporting within sectors. Law enforcement networks including Europol's SIENA[64] and INTERPOL's cybercrime platforms[65] facilitate intelligence exchange across jurisdictions. Cross-sector collaborations such as the APWG's eCrime Exchange[66] and the Global Signal Exchange enable real-time sharing of threat signals by technology and cybersecurity providers. Throughout the mobile communications industry, the GSM Association (GSMA)-run Telecommunication ISAC and High-Risk Number platform provide real-time means of exchanging fraud information.[67] Government programmes – from citizen reporting to public–private frameworks – extend intelligence and enforcement capacity. These platforms demonstrate how signal sharing multiplies force against coordinated criminal operations.

However, the ecosystem remains fragmented across organizational and jurisdictional boundaries. Government initiatives typically operate nationally; ISACs serve specific sectors; cross-sector collaboratives reach only participating members. Intelligence stays siloed due to interoperability gaps at multiple levels: inconsistent technical formats, divergent taxonomies and ontologies, variable trust between platforms and incompatible legal agreements. While standards such as Structured Threat Information Expression (STIX), Trusted Automated Exchange of Intelligence Information (TAXII) and Malware Information-Sharing Platform (MISP) enable technical exchange, semantic and governance barriers persist. Without more interoperable frameworks and clearing-house mechanisms that span technical, semantic and trust layers, critical intelligence falls through the gaps – slowing responses, limiting systemic impact and preventing those best positioned to act from receiving actionable signals.

## A call to scale and modernize signal sharing and abuse response

Addressing these coordination and interoperability challenges requires action in three dimensions: establishing shared standards and expectations for abuse reporting and intelligence exchange; building trust frameworks that enable responsible and active participation; and deploying advanced detection capabilities that match the scale of modern threats.

**Action 7 – Establish signal sharing as a core industry standard:** Signal sharing must become an established expectation and interoperable industry standard – underpinned by clear legal and governance frameworks that enable the responsible exchange of actionable intelligence across sectors and jurisdictions. Affected intermediaries, such as online platforms and financial institutions, should be legally authorized and incentivized to cooperate against scams and fraud based on well-governed indicators of suspicious activity. This includes the ability to share relevant information – such as account or infrastructure data – with government agencies and trusted partners for the narrow, legitimate purpose of detecting and preventing fraud.

As part of this effort, "trusted reporter" programmes can enhance the efficiency and reliability of abuse reporting. Under these programmes, organizations grant priority handling to reporters who consistently demonstrate accuracy and credibility, often through low false-positive rates and established one-to-one relationships. Such mechanisms illustrate how signal sharing can evolve from isolated exchanges into structured, high-trust partnerships that accelerate collective prevention and mitigation efforts.

Policy-makers should ensure that national and international legal frameworks explicitly permit privacy-preserving signal sharing between the public and private sectors, recognizing fraud prevention at scale as a matter of public interest. Clear safeguards and oversight mechanisms must protect the rights of individuals while enabling faster collective action against organized criminal networks. Establishing this shared foundation would transform fragmented initiatives into a cohesive, systemic defence capable of matching the scale and sophistication of modern online fraud.


> **Increasingly, online fraud is being driven by transnational criminal organizations that have access to great financial and technical resources, and operate across both online and offline environments. But we're making strong progress thanks to a multipronged approach, combining AI-boosted technical solutions and 'safety by design', awareness-raising and, crucially, cooperation with other industries and law enforcement to counter the scammers. Thanks to the great progress made in anti-scam technology and intel sharing, and ever-stronger collaborations across the impacted industries, we are increasingly able to disrupt the criminals and their operations.**
>
> Amanda Storey, Managing Director, Trust and Safety, Google

**Action 8 – Incentivize responsible conduct:** Sustained adoption of systemic defences requires incentives to align organizational behaviour with the public interest. Such incentives can take several forms and come from several sources. Regulators can set enforceable baselines and provide practical guidance; governance bodies such as ICANN and its stakeholders can raise contractual and accreditation standards; centralized reporting conduits such as NetBeacon Reporter, signal-sharing platforms like the Global Signal Exchange and industry associations such as the APWG can use their data to highlight high- and low-performing entities. Publicly recognizing strong actors and exposing laggards creates reputational incentives that complement regulatory and market drivers, shaping behaviour throughout the ecosystem. Incentive structures should reward the adoption of shared frameworks, participation in cooperative mechanisms and investment in preventive controls, while providing clear, measurable pathways for improvement. Transparency about performance – whether through public scorecards, certification programmes or regulatory reporting – drives accountability and enables informed decisions by users, partners and policy-makers. Success requires balancing recognition with enforcement, ensuring consequences for persistent non-compliance.

BOX 7 | **Signals in action: A case study for digital infrastructure reputation transparency**

The Global Signal Exchange (GSE) is a non-profit clearing house for the real-time, international, cross-sector sharing of scam and fraud threat signals. Established in January 2025 with 40 million threat signals, by October 2025 the GSE had grown to 550 million signals. More than 180 organizations have been onboarded or are in the pipeline, spanning major industry providers, technical and non-profit organizations and, now, government agencies: in September 2025, Singapore's Government Technology Agency became GSE's first government member.

GSE produces sector analysis that incorporates AI and machine learning tools and individually processes 1 million signals each day to create a dynamic threat score that is adjusted in real time through the community's feedback. The GSE enables both open and group sharing. Participants report that GSE signals are highly accurate, often unique and therefore immediately actionable.

Industry "league tables" are powerful tools to benchmark performance across categories of digital infrastructure providers. For example, GSE's Top Level Domain (TLD) league tables present the share of reported abuse relative to the size of each TLD provider, allowing comparison among similarly sized registries. The tables show that some providers maintain near-zero abuse rates while others have considerably higher rates – with the highest at 22.78%.[68] This creates visible incentives for best practice and public accountability.

**Action 9 – Implement AI-powered abuse screening during digital infrastructure enrolment and beyond:** Worsening levels of fraud and infrastructure abuse require detection capabilities matching their speed and sophistication. Traditional manual reviews or static checks can no longer keep pace with automated scams, large-scale domain abuse or identity spoofing. AI-powered shared services offer a scalable way to strengthen defences at the infrastructure layer by detecting and flagging malicious activity at the point of registration or onboarding. AI-powered systems should be built directly into digital infrastructure enrolment workflows to evaluate registration requests in real time. Such systems – potentially operated by existing consortia managing signal-sharing or abuse-reporting platforms – can analyse linguistic anomalies, infrastructure reuse patterns, behavioural signals, identity inconsistencies and reputation indicators to identify suspicious activity early. Privacy-preserving techniques (such as hashing, differential privacy and secure multiparty computation) can enable cross-provider detection while protecting user data. These systems should flag potential risks for human review, monitor post-enrolment activity for emerging threats and be refined continuously through feedback from shared abuse-intelligence networks.

> **At Microsoft, we're harnessing AI to stop fraud before it starts – protecting billions of digital interactions, shutting down 28 million fraudulent accounts and blocking $4 billion in fraud attempts in just the last 12 months. Using AI, our Central Fraud and Abuse Risk (CFAR) team's real-time detection and global partnerships are redefining what safety means in a digital world.**
>
> Kelly Bissell, Corporate Vice-President, Central Fraud and Product Abuse Risk, Microsoft

# Conclusion

## Stakeholders must work together to build a secure digital ecosystem for the future.

The digital infrastructure that enables modern life was never designed to bear the weight of organized criminal fraud at industrial scale. Yet the path forward is clear and within reach: shift the burden of security upstream to those best positioned to act, embed protection as the default rather than the exception and connect the fragmented efforts already under way into a coordinated global response. This is not about choosing between innovation and safety or between openness and accountability; it is about recognizing that operating digital infrastructure is a public trust, and that trust must be backed by responsibility.

At the same time, stronger defences must be built with appropriate safeguards – including transparent processes, effective appeal mechanisms and remedies for errors – ensuring that legitimate users are protected from both criminal abuse and from mistakes in well-intentioned security measures.

The actions outlined in this paper are achievable. Many are already in motion, supported by committed leaders across industry, government and civil society. What remains is to work together to build the digital ecosystem that's needed. The internet's early promise of connection and opportunity need not be abandoned; it can be renewed, secured and extended to all. Systemic defence is not just possible – it is already beginning to take shape. The momentum is building, and the time to act is now.

# **Appendix:** Glossary

**Access internet service provider (access ISP).** A company or organization that provides customers with access to the internet through broadband, mobile or other network connections. ISPs may also offer additional services such as email, web hosting or security features. Because they control the "last mile" to end users, ISPs play a role in filtering harmful traffic and bundling protective services, but their visibility into content is increasingly limited by encryption.

**Backbone internet service providers (backbone ISPs).** Large-scale telecommunications providers that operate the high-capacity backbone of the internet, interconnecting regional networks and routing global traffic. These Tier 1 providers serve as upstream infrastructure providers that typically view themselves as neutral conduits, responsible for performance and resilience rather than content or security. Criminals may exploit their neutrality and scale, but interventions usually occur downstream at access ISPs, resolvers or platforms.

**Content delivery networks (CDNs).** A distributed system of servers that cache and deliver web content (e.g. images, scripts, pages) from locations closer to end users. CDNs improve performance, availability and resilience. Many commercial CDNs are bundled with reverse-proxy services, which handle traffic to and from the origin server. Criminals can exploit these platforms to give malicious sites scale and legitimacy.

**Cyber-enabled fraud.** Fraud schemes in which criminals use digital technologies or online infrastructure to deceive victims and obtain money, goods, services or sensitive information. Unlike purely "cyber-dependent" crimes (such as ransomware or denial-of-service attacks), cyber-enabled fraud adapts traditional deception techniques to scale rapidly via the internet. It includes schemes that exploit email, messaging, websites, social media or payment platforms to impersonate trusted parties, misrepresent transactions or manipulate victims into authorizing transfers. Key mechanisms range from phishing and business email compromise to investment scams and online marketplace fraud. The defining characteristic is the use of digital channels as the primary enabler of deception and victimization, often blurring the boundaries between cybercrime and traditional fraud.

**Digital infrastructure services.** Systems, platforms and related resources that provide the essential functions of the internet – enabling the creation, exchange, authentication and delivery of data and online services. The term encompasses both the underlying infrastructure (e.g. networks, servers and security mechanisms) and the activities of providers who operate and maintain these capabilities for others. As described in the EU's NIS2 Directive, digital infrastructure services span nine categories, including domain name systems, trust services, data centres and content delivery networks.

**DNS abuse.** For the purposes of this paper, the intentional misuse of the DNS as *criminal infrastructure*, including the registration, compromise or manipulation of domain names to enable malicious activity – distinct from abusive content merely delivered through it.

**Domain name system (DNS).** The hierarchical, distributed system that translates human-readable domain names (e.g. example.com) into numerical IP addresses used by computers to identify and reach each other on the internet. The DNS functions as the internet's "phone book", directing user requests to the correct servers and enabling virtually all online activity. Because the DNS underpins routing and trust, criminals frequently misuse it by registering deceptive domains, hijacking records or manipulating lookups to support phishing, malware and other attacks.

**Email spoofing.** Term used to describe cybercriminals' practice of forging an email's "from" address to make messages appear to come from a legitimate organization or trusted sender.

**Internet protocol (IP) address.** A unique numerical identifier assigned to each device or server connected to the internet, used to route data between networks. IP addresses come in two formats – IPv4 (32-bit) and IPv6 (128-bit) – and function like digital street addresses, ensuring that information reaches the correct destination. Criminals may hide, spoof or rapidly change IP addresses (e.g. through fast-flux techniques) to evade detection and frustrate enforcement.

**Phishing.** A form of cyberattack or social engineering scam in which malicious actors impersonate trusted entities through fraudulent digital communications – typically emails, text messages or websites – to deceive victims into revealing sensitive information or performing actions that compromise security, often resulting in identity theft, financial fraud or unauthorized system access.

**Public key infrastructure (PKI).** A framework of digital certificates and trusted authorities that verifies identities and enables encrypted communication on the internet.

**Reverse proxy.** A service that sits in front of a website's origin server, handling all incoming requests and responses. Reverse proxies conceal the origin server's IP address and often terminate TLS/SSL sessions – meaning the user's encrypted connection ends at the proxy. The proxy then inspects or filters the traffic and may establish new encrypted connections to the original server. This allows the proxy to apply security features such as distributed denial of service (DDoS) attack mitigation, web application firewalls or traffic analytics. Most large providers also operate as CDNs, combining performance and security functions. Criminals have been observed exploiting these services to hide infrastructure, obtain free TLS certificates and frustrate takedown efforts.

**Smishing.** A form of **phishing** conducted through text messaging. The term originated from bad actors' use of short message service (SMS) texts for phishing – discussed elsewhere in this paper – but this term now applies to any text-based messaging protocol or platform.

**Transport layer security (TLS) certificates.** A digital credential (based on the X.509 standard) issued by a trusted certificate authority (CA) that verifies the identity of a website or service and enables encrypted communication using the TLS protocol. TLS certificates allow users' browsers or applications to confirm they are connecting to the intended domain and to establish a secure, encrypted session. Although these are often called "SSL certificates" in industry jargon, secure sockets layer (SSL) was the predecessor to TLS and is now obsolete; modern encrypted connections use TLS exclusively.

**Vishing.** A form of **phishing** conducted through voice calls or voicemail messages.

# Contributors

## Lead authors

### World Economic Forum

**Tal Goldstein**
Head of Strategy and Growth,
Centre for Cybersecurity

**Giulia Moschetta**
Initiatives Lead, Centre for Cybersecurity

### Institute for Security and Technology

**Taylor Grossman**
Director for Digital Security

**Steve Kelly**
Chief Trust Officer

**Tiffany Saade**
Adjunct Cyber and Artificial Intelligence Policy Fellow

**Jennifer Tang**
Associate for Cybersecurity and Emerging Technologies

# Acknowledgements

This white paper is the result of contributions from many experts and stakeholders, who shared their insights through community meetings, virtual and in-person workshops, events and one-to-one consultations, as part of the World Economic Forum's Partnership against Cybercrime initiative. The Forum would like to thank the following individuals for their valuable contributions:

**Jorij Abraham**
Global Anti-Scam Alliance

**Bushra Alahmadi**
Saudi Information Technology Company (SITE)

**Mick Baccio**
Splunk, a Cisco Company

**Sanjay Bahl**
Indian Computer Emergency Response Team (CERT-In)

**Abu Bakr**
BforeAI PreCrime

**Kerry-Ann Barrett**
Organization of American States (OAS)

**Cathrin Bauer-Bulst**
European Commission

**Alejandro Becerra**
Telefónica

**Jonathan Bellack**
Harvard University

**Kelly Bissell**
Microsoft

**Grant Bourzikas**
Cloudflare

**Graeme Bunton**
NetBeacon Institute

**Carolina Caeiro**
Global Signal Exchange

**Albert Calamug**
TikTok

**Peter Cassidy**
Anti-Phishing Working Group

**Jethro Cornelissen**
ING Group

**Leslie Daigle**
Global Cyber Alliance

**Conrad C. Daly**
World Bank Group

**Michael Daniel**
Cyber Threat Alliance

**Miguel De Bruycker**
Centre for Cybersecurity Belgium

**Stephane Duguin**
CyberPeace Institute

**Amr El Rahwan**
United Nations Office on Drugs and Crime (UNODC)

**Kemba Eneas Walden**
Paladin Capital Group

**Lotem Finkelsteen**
Check Point Software Technologies

**Simon Forster**
Quad9

**Jacky Fox**
Accenture

**Stewart Garrick**
Shadowserver Foundation

**Will Garrity**
Mastercard

**Alexandra Gerst**
Microsoft

**Chris Gibson**
Forum of Incident Response and Security Teams

**James Gill**
Banco Santander

**Rens Grim**
Global Anti-Scam Alliance

**Kate Grove**
National Crime Agency

**Joyce Hakmeh**
Chatham House

**Hila Hanif**
Amazon Web Services

**John Hauser**
EY

**Fred Heiding**
Harvard University

**Roman Huessy**
National Cybersecurity Centre (NSCS) Switzerland

**Attiqa Jaffri**
Zurich Insurance

**Terje Jensen**
Telenor

**Josh Kenway**
PayPal

**Emmanuel Kessler**
European Union Agency for Law Enforcement Cooperation (Europol)

**Samantha Kight**
GSM Association (GSMA)

**Olaf Kolkman**
Internet Society

**Timo S. Koster**
BforeAI PreCrime

**Aamir Lakhani**
Fortinet

**Jason Lancaster**
SpyCloud

**Matt LaVigna**
National Cybercrime Forensics and Training Alliance

**Luigi Lenguito**
BforeAI PreCrime

**Garry Lilburn**
Cyber Defence Alliance

**Polina Malaja**
Council of European National Top-Level Domain Registries (CENTR)

**Derek Manky**
Fortinet

**Gerry McQuaid**
Office of Communications (Ofcom)

**Cristiana Nador**
International Criminal Police Organization (INTERPOL)

**André Naumann**
Google

**Neil Parker**
Mastercard

**Paolo Pellegrino**
International Criminal Police Organization (INTERPOL)

**Andy Piazza**
Palo Alto Networks

**Philip Reitinger**
Global Cyber Alliance

**Humberto Luiz Ribeiro da Silva**
University of Brasilia

**Craig Rice**
Cyber Defence Alliance

**Jean-Jacques Sahel**
Google

**Jamie Saunders**
University of Oxford

**Rowena Schoo**
NetBeacon Institute

**Nick Seaver**
Deloitte

**Lavy Shtokhamer**
Standard Chartered Bank

**Sergey Shykevich**
Check Point Software Technologies

**Matthew Stith**
Spamhaus

**Laura Striegel**
Centre for Cybersecurity Belgium

**Mark Swift**
Trafigura Group

**Emily Taylor**
Global Signal Exchange

**Lucien Taylor**
Global Signal Exchange

**Syam Thommandru**
Zscaler

**Bruce Tonkin**
.au Domain Administration (auDA)

**Nicholas Tuppen**
Bank of America

**Peter Van Roste**
Council of European National Top-Level Domain Registries (CENTR)

**Nick Wenban-Smith**
Nominet

**Robin Wilton**
Internet Society

**Brett Winterford**
Okta

**Josephine Wolff**
The Fletcher School of Law and Diplomacy, Tufts University

**Jelena Zelenovic**
Matone European Investment Bank (EIB)

Additionally, the authors would like to acknowledge the following organizations and individuals for their feedback: UNODC's Regional Centre for Combatting Cybercrime and UNODC Global Programme on the Implementation of the Organized Crime Convention, Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)'s Names & Numbers Committee and Greg Aaron from Interisle.

## Production

**Bianca Gay-Fulconis**
Designer, 1-Pact Edition

**Alison Moore**
Editor, Astra Content

**Simon Smith**
Editor, Astra Content

# Endnotes


1. Netherlands National Coordinator for Counterterrorism and Security. (2022, October). *Netherlands National Cybersecurity Strategy*. https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028/TheNetherlandsCybersecurityStrategy2022-2028.pdf
2. The White House, Washington, DC. (2023, March). *US National Cybersecurity Strategy*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
3. UK Government Cabinet Office. (2021, December). *National Cyber Strategy 2022*. https://www.gov.uk/government/publications/national-cyber-strategy-2022
4. Global Anti-Scam Alliance (GASA). (2024). *2024 Global state of scams report*. https://www.feedzai.com/pressrelease/report-more-than-us1-trillion-lost-to-scams-in-one-year/
5. United Nations Development Programme (UNDP). (2025, May 21). *Anti-scam handbook v2.0*. https://www.undp.org/policy-centre/singapore/publications/anti-scam-handbook
6. World Economic Forum. (2025, January). *Global cybersecurity outlook 2025*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
7. European Union Agency for Cybersecurity (ENISA). (2025). *Threat landscape 2025*. https://enisa.europa.eu/publications/enisa-threat-landscape-2025
8. SlashNext. (2024, December 18). *SlashNext's 2024 phishing intelligence report shows credential phishing attacks increased by 703% in the second half of the year*. https://www.prnewswire.com/news-releases/slashnexts-2024-phishing-intelligence-report-shows-credential-phishing-attacks-increased-by-703-in-the-second-half-of-the-year-302334475.html
9. Heiding, F., Lermen, S., Kao, A., et al. (2024). *Evaluating large language models' capability to launch fully automated spear phishing campaigns: Validated on human subjects*. arXiv. https://arxiv.org/abs/2412.00586
10. Anti-Phishing Working Group (APWG). (2025). *Phishing activity trends report 2nd quarter 2025*. https://docs.apwg.org/reports/apwg_trends_report_q2_2025.pdf
11. News Service Bund. Le portail du Gouvernement suisse. (2025, July 29). *Cybercriminalité: Enquêtes internationales du MPC et de fedpol aboutissent à une condamnation pour Realtime-Phishing en Angleterre* [in French]. https://www.news.admin.ch/fr/newnsb/b4yhFXHLpERSkhgNMVb89
12. International Criminal Police Organization (INTERPOL). (2023, August 8). *Notorious phishing platform shut down, arrests in international police operation*. https://www.interpol.int/en/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation
13. United States Department of Justice. (2024, April 18). *Justice Department seizes four web domains used to create over 40,000 spoofed websites and store the personal information of more than a million victims*. https://www.justice.gov/usao-wdpa/pr/justice-department-seizes-four-web-domains-used-create-over-40000-spoofed-websites-and
14. European Union Agency for Law Enforcement Cooperation (Europol). (2024, April 18). *International investigation disrupts phishing-as-a-service platform LabHost*. https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost
15. INTERPOL. (2024, June 27). *USD 257 million seized in global police crackdown against online scams*. https://www.interpol.int/en/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams
16. Interisle. (2024, November 18). *Cybercrime supply chain 2024*. https://www.m3aawg.org/system/files/cybercrimesupplychain2024.pdf
17. NetBeacon Institute. (2025, August 13). *Recent spike in malicious phishing concentrated in two registrars*. https://netbeacon.org/recent-spike-in-malicious-phishing-concentrated-in-two-registrars/
18. Nosyk, Y., Korczynski, M., Maroofi, S., et al. (2024, November 8). *INFERMAL: Inferential analysis of maliciously registered domains*. https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf
19. Internet Corporation for Assigned Names and Numbers (ICANN). (2025, June 10). *Insights and clarifications on the INFERMAL study*. https://www.icann.org/en/system/files/files/insights-clarifications-infermal-study-10jun25-en.pdf
20. Interisle. (2024, July 23). *Phishing landscape 2024: An annual study of the scope and distribution of phishing*. https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing/
21. Deacon, A. (2023, August 14). *Use of subdomain providers gains popularity as a mechanism to launch phishing attacks*. https://oxil.uk/blog/use-of-subdomain-providers-gains-popularity-as-a-mechanism-to-launch-phishing-attacks
22. Ibid.
23. Interisle. (2025, September 7). *Phishing landscape 2025: A study of the scope and distribution of phishing*. https://interisle.net/insights/phishing-landscape-2025-an-annual-study-of-the-scope-and-distribution-of-phishing

24. ICANN. (n.d.). *Advisory: Compliance with DNS abuse obligations in the Registrar Accreditation Agreement and the Registry Agreement*. Retrieved October 27, 2025, from https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
25. Ibid.
26. ICANN. (2025, June 10). *Insights and clarifications on the INFERMAL study*. https://www.icann.org/en/system/files/files/insights-clarifications-infermal-study-10jun25-en.pdf
27. NetBeacon Institute. (2025, May). *White paper: Proposal for PDPs on DNS abuse*. https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf
28. Cloudflare (n.d.). *What is domain hijacking?* Retrieved October 27, 2025, from https://www.cloudflare.com/en-gb/learning/dns/what-is-domain-hijacking/
29. Subramani, K., Perdisci, R., & Skafidas, P. (2023, November 13). *Measuring CDNs susceptible to domain fronting*. arXiv. https://arxiv.org/pdf/2310.17851
30. Alcantara, J. M. (2024, May 23). *Phishing with Cloudflare workers: Transparent phishing and HTML smuggling*. Netskope. https://www.netskope.com/blog/phishing-with-cloudflare-workers-transparent-phishing-and-html-smuggling
31. Fortra. (2024, December 2). *Cloudflare's pages.dev and workers.dev domains increasingly abused for phishing*. https://www.fortra.com/blog/cloudflare-pages-workers-domains-increasingly-abused-for-phishing
32. US Federal Bureau of Investigation. (2025, May 29). *Infrastructure used to manage domains related to cryptocurrency investment fraud scams between October 2023 and April 2025*. https://www.ic3.gov/CSA/2025/250529.pdf
33. US Department of the Treasury. (2025, May 29). *Treasury takes action against major cyber scam facilitator* [press release]. https://home.treasury.gov/news/press-releases/sb0149
34. US Federal Bureau of Investigation. (2025, May 29). *Infrastructure used to manage domains related to cryptocurrency investment fraud scams between October 2023 and April 2025*. https://www.ic3.gov/CSA/2025/250529.pdf
35. Rice, S. (2025, April 29). *UK bans SIM farms to tackle telecoms crime and cyber fraud*. Cyber Magazine. https://cybermagazine.com/network-security/uk-bans-sim-farms-as-vodafone-blocks-73-5m-scam-texts
36. Meyers, A. (2025, February 27). *CrowdStrike 2025 global threat report: Beware the enterprising adversary*. CrowdStrike Blog. https://www.crowdstrike.com/en-us/blog/crowdstrike-2025-global-threat-report-findings/
37. Keepnet. (2024). *The 2024 voice phishing (vishing) response report*. https://keepnetlabs.com/reports/2024-voice-phishing-response-report
38. Guo, S. (2025, July 8). *RCS messaging loophole exposes global users to smishing attacks*. https://btw.media/all/internet-governance/rcs-messaging-loophole-exposes-global-users-to-smishing-attacks/
39. Walsh, P. (2025, February 2025). *Why SMS phishing is out of control – and the only real solution that can stop it*. https://paul-walsh.medium.com/why-sms-phishing-is-out-of-control-and-the-only-real-solution-that-can-stop-it-47456116220c
40. The systemic approach presented in this white paper aligns with the broader framework against fraud that will be detailed in the forthcoming *UNODC Public-Private Partnership Toolkit Against Organized Fraud* (to be released in 2026).
41. DNS Research Federation. (n.d.). *500k domain names*. Retrieved October 27, 2025, from https://dnsrf.org/research/safest-tld-league-/safest-tlds---all-tables/tld--500k/index.html
42. ICANN. (2012, February 25). *SSAC comment on the orphan glue records in the draft applicant guidebook*. https://www.icann.org/groups/ssac/documents/sac-048-en
43. ICANN. (2024). *2024 global amendments to the 2013 Registrar Accreditation Agreement (RAA) and Base gTLD Registry Agreement (Base RA)*. https://www.icann.org/resources/pages/global-amendment-2024-en
44. ICANN. *Advisory: Compliance with DNS abuse obligations in the Registrar Accreditation Agreement and the Registry Agreement*. https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
45. ICANN. (n.d.). *All you need to know about ICANN Domain Metrica*. Retrieved 2025, October 27, from https://www.icann.org/en/system/files/files/domain-metrica-brochure-20may25-en.pdf
46. ICANN. (n.d.). *Welcome to the INFERMAL Project*. Retrieved 2025, October 27, from https://www.icann.org/resources/pages/inferential-analysis-maliciously-registered-domains-infermal-2024-12-03-en
47. ICANN. (2025, July 31). *DNS abuse small team report to GNSO Council*. https://gnso.icann.org/sites/default/files/policy/2025/draft/dns-abuse-small-team-report-04aug25-en.pdf
48. ICANN. (2025, June 16). *GAC advice*. https://gac.icann.org/advice/itemized/202506-16-policy-development-related-to-dns-abuse
49. NetBeacon Institute. (2022, December 6). *Best Practice: Anti-fraud tools and registration flows for registrars*. https://netbeacon.org/best-practice-anti-fraud-tools-and-registration-flows-for-registrars/
50. ICANN. (2025, June 10). *Insights and clarifications on the INFERMAL study*. https://www.icann.org/en/system/files/files/insights-clarifications-infermal-study-10jun25-en.pdf

51. Global Anti-Scam Alliance. (2023). *Ten recommendations to turn the tide on online scams*. https://www.gasa.org/turning-the-tide-on-scams

52. Council of European National Top-level Domain Registries (CENTR). (2022). *CENTR publishes white paper on registration data accuracy in European national domain registries*. https://www.centr.org/news/news/data-accuracy-paper.html

53. European Union (2022, December 27) *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

54. European Commission. (2025, May 5). *eIDAS regulation*. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

55. World Economic Forum. (2025, July 10). *Advancing systemic defence: What cyber leaders say about fighting phishing and fraud*. https://www.weforum.org/stories/2025/07/rethinking-cybersecurity-a-systemic-approach-to-combat-cyber-enabled-fraud-and-phishing/

56. United Nations Office on Drugs and Crime (UNODC). (2024). *United Nations Convention against Cybercrime*. https://www.unodc.org/unodc/cybercrime/convention/home.html

57. Abrams, L. (2019, August 14). *Chrome and Firefox changes spark the end of EV certificates*. BleepingComputer. https://www.bleepingcomputer.com/news/software/chrome-and-firefox-changes-spark-the-end-of-ev-certificates/

58. Safeonweb.be. (n.d.). *Safeonweb browser extension*. Retrieved October 27, 2025, from https://safeonweb.be/en/safeonweb-browser-extension

59. Europol (2025, October 27) *Position paper on caller ID spoofing*. https://www.europol.europa.eu/publications-events/publications/position-paper-caller-id-spoofing

60. GSM Association (GSMA). (2025, 29 April). *Baseline security controls version 5.0*. https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2025/06/FS.31-Baseline-Security-Controls-v5.0.pdf

61. Fido Alliance. (2024, September 14). *White paper: Displace password + OTP authentication with passkeys*. https://fidoalliance.org/white-paper-displace-password-otp-authentication-with-passkeys/

62. Finnish Transport and Communications Agency (TRAFICOM). (n.d.). *SMS sender ID*. Retrieved October 27, 2025, from https://www.traficom.fi/en/communications/broadband-and-telephone/sms-sender-id

63. NetBeacon Institute. (n.d.). *NetBeacon reporter*. Retrieved October 27, 2025, from https://netbeacon.org/reporting/

64. Europol. (2025, August 13). *Secure Information Exchange Network Application (SIENA)*. https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena

65. INTERPOL. (n.d.). *Cybercrime collaboration services*. Retrieved October 27, 2025, from https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services

66. Anti-Phishing Working Group. (n.d.). *The APWG eCrime eXchange (eCX)*. Retrieved October 27, 2025, from https://apwg.org/ecx

67. GSM Association (GSMA). (n.d.). *T-ISAC*. Retrieved October 27, 2025, from https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/

68. Global Signal Exchange. (2025). *League tables*. https://www.globalsignalexchange.org/leaguetables

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org