bilingual edition

ptsoc {news}

18

Cybersecurity in the Lusophone World: Preparedness and Cyber Threats*

3 questions to António Ribeiro, Head of Cybersecurity at Minsait in Portugal (Indra Group)

European Cybersecurity Month: #THINKB4UCLICK

*With contributions from: Angola, Brazil, Cape Verde, Mozambique and Portugal

.pt

Cybersecurity in the Lusophone World: Preparedness and Cyber Threats

According to the latest Global Cybersecurity Index released by the ITU, "cyberattacks are considered the fifth most likely risk to trigger a major global crisis." As this is a cross-cutting risk that affects all countries and regions, we could assume that the Lusophone world is not substantially different from the rest of the world in terms of vulnerabilities to cyberattacks and cyber risks in general.

However, while there are no indicators suggesting that there are more threats in Lusophone countries than elsewhere, one significant factor regarding vulnerability relates to each country's degree of preparedness to face such threats.

The same ITU report defines several levels ("tiers") of national preparedness, which are worth exploring to better understand the situation across the Lusophone space:

Level 1 (T1) – "Role-modelling": countries scoring at least 95/100 on the Global Cybersecurity Index metrics, demonstrating a strong national commitment to cybersecurity through coordinated, government-driven actions that include the assessment, establishment, and implementation of generally accepted cybersecurity measures across all five pillars, or even all.[1]

Level 2 (T2) – "Advancing": countries scoring at least 85/100, showing strong commitment to cybersecurity with government-led coordinated measures covering four pillars at most, or a substantial number of indicators.

Level 3 (T3) – "Establishing": countries scoring at least 55/100, reflecting a basic commitment to cybersecurity through government-driven actions involving the assessment, establishment, or implementation of generally accepted measures across a moderate number of pillars or indicators.

Level 4 (T4) – "Evolving": countries scoring at least 20/100, showing a basic level of commitment through government-led actions covering at least one cybersecurity pillar or several indicators/subindicators.

Level 5 (T5) – "Building": countries scoring below 20/100, demonstrating a very basic level of cybersecurity commitment through government-led actions covering at least one indicator and/or subindicator.

According to this model, Portugal and Brazil are classified as Level 1 countries, while among

[1] According to the ITU methodology, these five pillars are: Legal measures; Technical measures; Organisational measures; Capacity-building measures; and Cooperation measures.

Foto: PP Creative adobe stock

the remaining PALOP nations, Mozambique ranks highest in preparedness, at Level 3.

Investment and Training

The need for greater investment — both at the state and enterprise levels — alongside training initiatives for citizens in general and workers in particular, is a point of consensus among institutional and governmental representatives who attended the recent Lusophone Internet Governance Forum held in Maputo last September (see "Maputo Letter").

João Tomar, board member of ARME (Multisectoral Regulation Agency of the Economy) of Cape Verde, told PTSOC News that ARME "advises companies and institutions to invest in their staff, to train them, and to invest in software for early virus and threat detection".

ARME manages both the .CV domain and the country's public key infrastructure. João Tomar noted that the Cape Verdean government "has adopted digitalization as a public policy and a priority investment," also as a means of attracting data center investments and digital nomads.

For these projects, Cape Verde has also relied on World Bank investments. "In today's digital world, without trust, without security, there is no business," concludes João Tomar.

Phishing and Ransomware

The most common attack vector across all Lusophone countries is phishing, often associated with ransomware.

Professor Lourino Chemane, Chairman of the Board at INTIC – National Institute of Information and Communication Technologies of Mozambique, identifies phishing as the main attack vector in Mozambique, "mainly targeting Internet-accessed electronic payment systems provided by banks and telecommunications operators, particularly in urban centers." This includes mobile wallets offered by telecom providers, covering a user base of about 19 million people in areas with network coverage.

Chemane also highlights "scams involving people asking for money via SMS, WhatsApp, and social networks," as well as email, phone, or other telecommunication-based phishing schemes "aimed at stealing data, passwords, inducing transfers, or prompting users to click on malicious links."

André Pedro, Director of INFOSI – National Institute for the Promotion of the Information Society of Angola, confirms that "phishing is the leader among all [cyberattack vectors]" in the country and identifies social networks as one of the main sources of such threats. These are messages, he explains, "targeted at end users, such as 'update your account,

The Maputo Letter

The organizers of the 3rd Lusophone Internet Governance Forum approved a final document - the "Maputo Letter"- which "invites Lusophone countries and their active communities to mobilize civil society, the technical community, academic researchers, and business sectors that develop, produce, market, and use the Internet and digital services, to engage with their respective governments, at all levels, in multistakeholder processes to discuss regulatory proposals concerning the use of social media platforms, artificial intelligence, cybersecurity, privacy and data protection, and digital governance."

The document also recognizes that "capacity-building in Internet Governance among Lusophone countries is crucial for consolidating models based on multistakeholder principles, encompassing global topics such as artificial intelligence, cybersecurity, personal data protection, and data governance — toward a systemic vision for building a more resilient, secure, and trustworthy Lusophone digital ecosystem. Exchanges between Local Forums and Youth Programs within the Lusophone Internet Governance ecosystem will represent valuable contributions."

The full document can be accessed at https://igf-lusofonia.pt/carta-de-maputo.

Foto: Delta Amphule, adobe stock

we'll help you' or 'if you're having trouble receiving receipts…'."

Meanwhile, Rodolfo Avelino, Advisor to the Brazilian Internet Steering Committee (CGI.br), admits that many incidents go unreported, "but among the reported ones, ransomware remains the most common—and in many cases, the attack vector is also phishing—whether through email or some other form of user interaction."

According to these three officials, in all these countries, the key to mitigating these attacks lies largely in training initiatives promoted by the respective national institutions, targeting both end users and businesses.

Lourino Chemane also emphasizes his government's efforts to increase the country's digital resilience, including investments in robust legal and regulatory frameworks, improved interoperability between public entities, the private sector, academia, and civil society, among other measures.

Portugal: Incidents Up 36%

In Portugal, the National Cybersecurity Center (CNCS) has just published the 6th edition of its Risks and Conflicts Report, revealing a 36% increase in cybersecurity-related incidents in 2024 compared to the previous year.

Lino Santos, CNCS Coordinator—also present at the Maputo event—confirms that the

Digital Capacity-Building Project

LusNIC, the association that brings together all top-level domain (ccTLD) registries of the Lusophone world, in partnership with ICANN's Coalition for Digital Africa, is developing a digital capacity-building project aimed at its African members (.cv, .ao, .st, .gw, and .mz). The initiative runs until March 2026 and represents a strategic step toward consolidating the technical, legal, and operational capabilities of these registries.

According to Marta Moreira Dias, President of LusNIC and Board Member of .PT, "supporting and collaborating with our peers in the Lusophone world has always been a priority for .PT — not only as a founding member of LusNIC, but also as the national ccTLD manager, working daily toward building a more open, transparent, secure, and resilient Lusophone digital space."

This project includes online and in-person training sessions, based on a tailored assessment of each ccTLD's training needs, the development of business plans adapted to each country's context, and the translation of key reference materials into Portuguese.

The first training session took place on September 24 in Mozambique, integrated into the Lusophone Internet Governance Forum program, and featured five panels with six .PT trainers.

In total, the project includes four training sessions — two in-person and two online — scheduled through February 2026. Each session will be adapted to the realities and priorities of each country, ensuring practical impact and alignment with the region's digital development goals.

Foto: hdesert, adobe stock

main concerns "relate to phishing schemes associated with all types of scams, i.e., social engineering instruments perpetrated by organized cybercrime actors."

Equally worrying, he adds, are "identity and data theft incidents stemming from a phenomenon known as Info Stealer, a type of malware that primarily affects mobile devices—but also computers—exfiltrating all personal data related to home banking access, email accounts, personal or professional notes, as well as social media and browser profiles. In essence, our entire digital footprint is exfiltrated by these criminals, then packaged, quantified, and monetized on the Dark Web."

"This concerns us not only due to personal data protection breaches but also because this rise represents a critical steppingstone and enabler for other types of attacks, such as ransomware—using valid credentials acquired on the Dark Web as an entry point into organizational infrastructures," Santos explains.

The Role of DNS Server Administrators

José Casinha, Board Member of .PT, argues that DNS server administrators should play "a crucial role in mitigating risks associated with attacks such as phishing, smishing, and pharming by implementing technical and operational mechanisms that reinforce the integrity and resilience of the system."

"Among the priority measures," he explains, "is the implementation of DNSSEC, which ensures the authenticity of DNS responses and prevents malicious redirects." He also recommends using DNS over TLS (DoT) and DNS over HTTPS (DoH) to protect the confidentiality and integrity of DNS queries. "Policies such as rate limiting and Response Policy Zones (RPZ) make it possible to block malicious domains and reduce the impact of amplification attacks."

For José Casinha, "DNS record hygiene is essential: unauthorized changes must be monitored, administrative access should be restricted with multifactor authentication, and audit logs must be maintained. In combating email phishing, it is crucial to properly configure and monitor SPF, DKIM, and DMARC, preventing the fraudulent use of domains."

Moreover, "servers should be segmented and isolated, with strict zone transfer controls and tested backup and recovery mechanisms. Continuous DNS traffic monitoring, supported by threat intelligence feeds, enables the detection of anomalous patterns and suspicious domains in real time."

"Finally," Casinha concludes, "DNS security must be complemented by team training and active reputation monitoring of domains, ensuring comprehensive protection against manipulation and digital fraud".

3

António Ribeiro

Head of Cybersecurity at Minsait in Portugal (Indra Group)

1. Most cybersecurity problems and challenges are transversal. In the case of the PALOP countries, are there specific national challenges?

Despite the differences between countries, the PALOP nations share common cybersecurity challenges. Technological infrastructures are often fragile or outdated, limiting incident response capabilities. Investment in digital security remains low, reflected in the scarcity of appropriate tools and the absence of robust national strategies. The lack of skilled professionals, coupled with limited continuous training programs, further increases organizational vulnerability. Moreover, low digital literacy and limited public awareness of cyber risks make the human factor one of the primary risk vectors.

Each country also presents its own specificities: Angola faces a high number of attacks, particularly in the education and healthcare sectors, with over 250 intrusion attempts per day, mainly ransomware and phishing; Mozambique leads the PALOP countries in cybersecurity maturity, according to the ITU report published in September 2024; Cape Verde has made significant progress through the creation of a National Communications Agency and a National Cybersecurity Strategy, but still needs to strengthen its digital resilience; Guinea-Bissau and São Tomé and Príncipe display the lowest levels of preparedness, with limited resources and high exposure to threats. These contexts highlight the need for tailored strategies, investment in local capacity, and regional cooperation.

At the regional level, Africa still lacks a centralized coordinating entity capable of defining policies, regulating, certifying, and coordinating cooperation among states like ENISA in Europe. However, ongoing efforts in this direction will certainly benefit the PALOP countries.

Foto: Rocha Santos, adobe stock

2. Many cybersecurity problems can be mitigated through proper investment in concrete measures (hardware, software, training…). To what extent are organizations in fragile economies more vulnerable to cyber threats?

Cybersecurity is one of the fundamental pillars of digital resilience. Yet in fragile economies, limited financial and human resources hinder consistent investment in essential measures such as robust infrastructure, updated software, and, most importantly, continuous staff training. This reality makes these organizations more vulnerable to attacks that exploit their weaknesses.

In the PALOP region, although positive signs are emerging, technical and human capacity development remains a critical challenge for most countries. It is in this context that Minsait adapts its response to each organization's security challenges, sector, and maturity level. Companies with international presence and experience in environments of varying digital maturity — like Minsait — have been supporting these economies through integrated approaches combining technology, managed services, and continuous training. The goal is clear: to ensure that digital protection is not a privilege, but a foundational element of sustainable and secure development.

3. In recent years, ransomware has become one of the most critical cybersecurity issues, often driven by social engineering. Is the human factor — and, specifically, employee training — a bigger challenge in these regions compared to Western countries?

The human factor remains, undeniably, an organization's first line of defense. The exponential rise of ransomware—often initiated through social engineering techniques such as phishing—reinforces the importance of ongoing training and awareness among employees and the public.

Social engineering succeeds when tailored to the target's context and when the target is appealing to the attacker, whether for financial or other reasons. Thus, attackers not only operate within their local markets but also increasingly export their tactics to more profitable targets, such as the European market.

In the PALOP region, this challenge is evident. The shortage of qualified professionals, limited access to specialized technical training, and low digital literacy levels hinder the creation of a strong cyber-security culture. Although comprehensive data is still lacking for all countries in the region, most continue to face structural difficulties in digital education and technical training, increasing vulnerability to social engineering–based attacks.

Even so, progress is being made. Capacity-building initiatives by universities, multilateral organizations, and tech companies are gaining momentum. In this context, cybersecurity solutions that integrate both technology and awareness components play a strategic role. Organizations with experience in digitally diverse environments, such as Minsait, have been working to transfer knowledge and strengthen local skills.

The best technology in the world will always fall short if users are not prepared to recognize and avoid common threats. This is precisely where the greatest challenge — and opportunity — for the PALOP countries lies.

European Cybersecurity Month: #THINKB4UCLICK

"Think Before U Click" has been, since 2020, the motto of the European Cybersecurity Month (ECSM)—an initiative by the European Union Agency for Cybersecurity (ENISA) and the European Commission, coordinated in Portugal by the National Cybersecurity Center (CNCS).

The campaign's goal is to promote cybersecurity awareness among EU citizens and organizations, providing up-to-date information on online safety through education and best-practice sharing.

Every October, hundreds of events take place across Europe, including conferences, workshops, training sessions, webinars, and presentations, to promote digital safety and cyber hygiene, especially among EU citizens.

In 2025, ENISA continues to coordinate the campaign, acting as a hub for all EU Member States and institutions, fostering expert collaboration, synergy, and unified messaging among citizens, businesses, and public administrations.

The rise of phishing – A thorn in my (web)site

According to ENISA, phishing remains the leading initial intrusion vector, responsible for around 60% of cases and continuing to be an effective technique for executing cyberattacks.

Phishing can take many forms, such as fake CAPTCHA prompts on compromised or fraudulent websites, tricking users into executing commands under the guise of human verification.

Additionally, Phishing-as-a-Service (PhaaS) platforms have emerged, automating the generation of phishing kits by cloning login pages and distributing malicious links. These enable cybercriminals and threat actors to impersonate trusted companies and brands to deceive users.

Worse yet, AI tools, particularly LLMs, are increasingly used to craft more convincing phishing emails. By early 2025, AI assisted phishing campaigns accounted for over 80% of all observed social engineering activity worldwide.

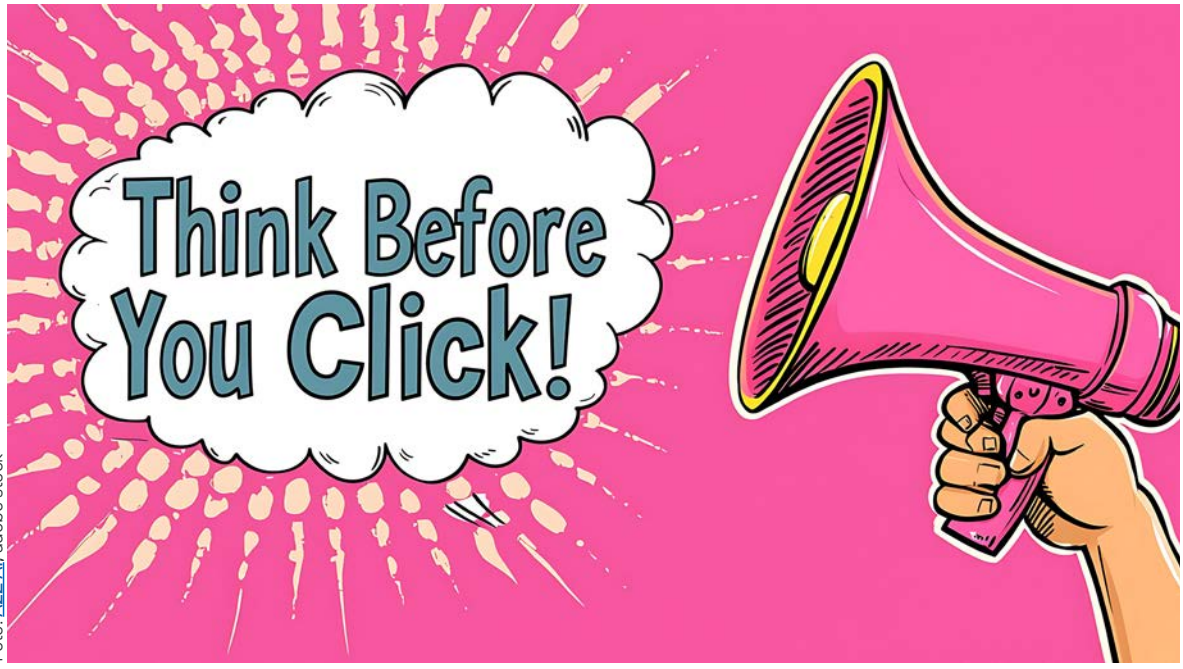

Foto: A2Z AI, adobe stock

For this reason, ENISA has used October's initiatives to urge all users to stay alert to the diverse forms of phishing and cyber fraud, including:

- Phishing – email-based phishing
- Quishing – QR-code phishing
- Spearphishing – targeted phishing
- Smishing – SMS-based phishing
- Vishing – voice-based phishing
- Whaling – executive-level phishing
- BEC – business email compromise schemes
- Deepfakes – AI-based frauds

As in previous years, the month was marked by numerous initiatives and the publication of reports and studies—valuable sources of information and prevention in the cybersecurity domain.

Separately from ECSM, it is worth noting that the CNCS offers free online courses in e-learning format, helping citizens develop the knowledge needed to become more informed and resilient against cyber threats—both in daily life and in the workplace.

These courses, available through the NAU platform, cover topics such as cyber hygiene, disinformation, online shopping security, and social media safety. All four remain free to access until December 18, 2025.

ENISA Threat Landscape October 2025

The latest ENISA Threat Landscape Report (2025) shows that threat groups are reusing tools and techniques, introducing new attack models, exploiting vulnerabilities, and collaborating to compromise the security and resilience of the EU's digital infrastructures.

Based on a threat-centric approach and contextual analysis, the study examined 4,875 incidents between July 1, 2024, and June 30, 2025.

Key findings include:

- Ransomware remains the most impactful threat in the EU.
- Hacktivism surged, accounting for nearly 80% of all incidents, mainly through low-impact DDoS campaigns targeting EU Member State websites, though only 2% caused service disruptions.

- State-aligned threat actors intensified operations against EU organizations. "Annexed" state actors engaged in cyber espionage targeting public administration sectors, while EU citizens faced Foreign Information Manipulation and Interference (FIMI).
- Phishing (60%) and vulnerability exploitation (21.3%) were the two main intrusion vectors.

Risks and Conflicts Report 2025

Portugal's National Cybersecurity Center released, in late September, the 6th edition of its *Risks and Conflicts Report*, revealing that in 2024, the number of cybersecurity incidents rise significantly, in a year marked by a high incidence of phishing and smishing attacks, other forms of social engineering, vulnerability exploitation, distributed denial-of-service (DDoS), and, most notably, ransomware.

According to the report, "the most relevant incidents in 2024 were primarily related to malicious code in the broadest sense, particularly ransomware and infostealers, which impacted the country in a year characterized by multiple credential leaks."

QUADRO DE AMEAÇAS: CIBERAMEAÇAS/AGENTES DE AMEAÇA CRÍTICOS EM PORTUGAL, 2024/2025

TOP 10 - Ciberameaças/ TOP 3 - Agentes de ameaça	Cibercriminosos	Agentes Estatais	Hacktivistas
Phishing e *Smishing*			
Engenharia Social e Burlas *Online*			
Ransomware			
Exploração de Vulnerabilidades			
Negação de Serviço Distribuída (DDoS)			
Comprometimento de Contas			
Código Malicioso			
Exfiltração de informação			
Ciberespionagem			
Tentativa de *Login*			

Agentes de ameaça e ciberameaças com relevância elevada em Portugal durante 2023/2024.
Agentes de ameaça e ciberameaças com relevância média em Portugal durante 2023/2024.
Ciberameaça com frequência elevada como prática dos agentes de ameaça em causa em Portugal.
Ciberameaça com frequência média como prática dos agentes de ameaça em causa em Portugal.
Ciberameaça com frequência baixa ou inexistente como prática dos agentes de ameaça em causa em Portugal.

Fonte: CNCS

State of AI in Telecommunications: 2025 Trends

NVIDIA published its third annual report on The State of AI in Telecommunications, revealing that 97% of telecom sector respondents are evaluating or adopting AI to enhance customer experience, employee productivity, network operations, cost reduction, and new business opportunities.

Respondents were split between active AI implementation and pilot testing, with 49% already using AI and another 49% in trial or assessment phases. Those not using or planning to use AI dropped from 10% in 2023 to just 3% in 2024.

The State of Broadband in Africa

The ITU, the UN's digital technologies agency, published in September its report The State of Broadband in Africa, providing an overview of the continent's mobile coverage progress.

In countries with mature cellular networks, 2G has been discontinued, and 3G networks are being phased out. According to the report, by the end of 2024, just over half of all mobile connections in Africa were still 3G, and 10% of users continued using 2G.

Nevertheless, 4G coverage grew to one-third of all connections, and while 3G usage is expected to decline as 4G expands, 5G coverage is projected to reach only 17% penetration by 2030.

This publication is produced by .PT

Editor
António Eduardo Marques

Graphic Design
Sara Dias
Maria Cristóvão

Photography
Capa: smalltinykid, adobe stock
Índice e contracapa: Jason Yoder, adobe stock

Quarterly publication
October 2025


.pt
www.pt.pt