Cybersecurity Threat Report 2026

CERT-MU

March 2026

Contents

1. Introduction

The global cyber threat landscape continues to evolve at an unprecedented pace, driven by rapid digitalisation, increasing geopolitical tensions, and the accelerated adoption of emerging technologies such as artificial intelligence. In 2025, cyber threats grew not only in volume but also in sophistication, impact, and intent, affecting governments, critical infrastructure, private-sector organisations, and citizens worldwide.

Cyber incidents observed throughout 2025 demonstrated a clear shift towards more destructive, disruptive, and financially motivated attacks. Ransomware operations became more targeted and professionalised, supply chain compromises amplified systemic risk, and the abuse of artificial intelligence lowered the barrier for cybercrime while increasing the realism of fraud, social engineering, and malicious content. At the same time, digital platforms continued to be misused to facilitate illegal activities, disinformation, and serious violations of privacy, often beyond the effective reach of national authorities.

At the national level, Mauritius has not been immune to these evolving threats. Throughout 2025, increased cyber activity was observed targeting public institutions, critical information infrastructures, businesses, and individuals. Incidents ranged from phishing and online fraud to ransomware attempts, data breaches, and the misuse of digital platforms for criminal and harmful activities. The growing digital footprint of the country, coupled with increased reliance on online services and interconnected systems, has further expanded the attack surface. These developments underline the importance of strengthening national cyber resilience, enhancing incident reporting and response mechanisms, and fostering closer collaboration among government entities, law enforcement, the private sector, and civil society.

This report provides a comprehensive overview of the cyber threat landscape in 2025, highlighting major trends, threat actor behaviours, and vulnerabilities that shaped the year, both globally and within the Mauritian context. It also examines some of the most impactful cyberattacks recorded in 2025, illustrating how cyber operations can lead to widespread operational disruption, economic losses, and harm to individuals and society at large.

Building on these observations, the report presents forward-looking assessments and predictions for 2026, identifying emerging threats, anticipated attacker tactics, and key risk areas that organisations and policymakers must prepare for. The aim is to support informed decision-making, enhance cyber resilience, and encourage proactive risk management across sectors.

As cyber threats continue to transcend borders, sectors, and technologies, this report underscores the importance of collective responsibility, timely information sharing, and coordinated national and international responses to safeguard Mauritius' digital ecosystem in 2026 and beyond.

2. Most Impactful Global Cyber Incidents 2025

2025 has been another tumultuous year for cyber security, with a number of high-profile breaches and incidents making headlines around the world. From state-sponsored cyber-attacks to extortion campaigns, it is clear that the threat landscape is constantly evolving. Cybersecurity professionals faced new challenges, doing battle deep in the trenches to proactively prevent the next big event. Let's take a look back at the biggest cyberattacks, threats, and data breaches to rock the world in 2026.

a) The 16 Billion Credential "Mega Leak" – Largest Password Exposure in History

In 2025, researchers at Cybernews uncovered 30 exposed datasets containing more than 16 billion login credentials. These included passwords for Google, Apple, Facebook, Telegram, GitHub and even government services. While there was no single breach of those big tech firms, the dataset was a massive aggregation of credentials stolen by infostealer malware and earlier breaches. Hosted openly online for a period, it effectively turned into a "credential buffet" for attackers. Analysts and media quickly dubbed it a historic data leak, warning that the compilation itself was as dangerous as any one breach because it enabled industrial-scale credential stuffing and account takeover.

b) Collins Aerospace vMUSE Airport Systems Ransomware Attack

In March 2025, a ransomware attack on Collins Aerospace's vMUSE platform caused widespread disruption across European aviation. vMUSE is used by airports for passenger check-in and boarding, and the attack forced airlines to revert to manual processes for passenger management and baggage handling.

Operations were disrupted at more than 20 airports, including Heathrow, Frankfurt, and Amsterdam Schiphol, leading to thousands of flight delays and cancellations. British police arrested a man in connection with the investigation under the Computer Misuse Act, although the responsible criminal group has not been publicly confirmed. In response, the European Aviation Safety Agency issued urgent guidance on third-party risk management and resilience planning for airport IT systems.

The vMUSE attack highlighted the fragility of shared critical systems and the cascading impact of vendor failures. It reinforced the importance of redundancy, real-time threat monitoring, and stronger oversight of third-party technology in the aviation sector.

c) Marks & Spencer and the UK Retail Ransomware Campaign

In April 2025, a coordinated ransomware campaign was launched against major UK retailers, including Marks & Spencer, the Co-op, and Harrods. The attack dominated headlines for weeks and set the tone for a year marked by supply chain exploitation and cross-sector exposure. The attackers, linked to the Scattered Spider group, used sophisticated social engineering techniques to compromise a third-party service provider. From there, they were able to

infiltrate multiple retail networks, deploy tailored ransomware payloads, exfiltrate customer data, and issue extortion demands aimed at preventing public disclosure.

The financial impact was severe. Marks & Spencer reported that pre-tax profits fell from £391.9 million to just £3.4 million in the six months to 27 September. Online sales platforms, payment systems, and gift card services were unavailable for weeks, while the Co-op experienced major supply chain disruption and Harrods faced checkout outages and logistics delays. A cross-sector investigation led by the National Crime Agency resulted in multiple arrests and placed a sharp spotlight on weaknesses in third-party access management across the retail industry.

This campaign demonstrated how shared vendors and cloud integrations can expose entire sectors to a single point of failure. It accelerated the push toward Zero Trust architectures, stricter vendor onboarding, and stronger ransomware resilience across retail supply chains.

d) St. Paul Municipal Systems breach

In July 2025, the city of St. Paul, Minnesota, declared a state of emergency following a ransomware attack that disabled key municipal systems. The attack, attributed to the Interlock group, compromised a shared network drive and encrypted systems responsible for billing, emergency coordination, and citizen services. City hall and public offices were offline for more than two weeks, prompting federal assistance and support from the US National Guard's cyber unit. The incident reignited debate around chronic underinvestment in local government IT infrastructure and cyber resilience.

The St. Paul breach exposed how legacy systems and delayed patching leave civic infrastructure highly vulnerable. It underlined the need for modernisation, Zero Trust controls, and regular cyber resilience exercises at local government level.

e) SalesLoft data breach and third-party compromise

In July 2025, one of the most far-reaching supply chain incidents was centred on SalesLoft, a widely used sales engagement platform integrated with Salesforce. Threat actors exploited OAuth integrations to gain access to customer environments at scale. Among the affected organisations was TransUnion, which disclosed the exposure of personal data belonging to 4.46 million US consumers. Other impacted organisations included Google, Workday, Farmers Insurance, Chanel, and Qantas. Security analysts linked the campaign to ShinyHunters operating alongside groups such as Scattered Spider, reflecting a growing trend toward extortion models that prioritise high-value integrations over individual targets.

The SalesLoft breach illustrated how trusted SaaS integrations can become powerful attack vectors. It has driven renewed scrutiny of OAuth permissions, identity security, and third-party application governance.

f) Change Healthcare Ransomware Breach

In early 2025, Change Healthcare, a unit of United Health's Technology was hit by a ransomware attack. The attack was linked to the ALPHV/BlackCat group. Further to this attack, Change Healthcare suffered prolonged outages that disrupted pharmacy claims, clinical workflows and billing across the United States. The company was also slammed globally for apparently making a ransom payment, with the attack becoming a case study on why negotiating with criminals is never a good idea.

The attack had a massive knock-on effect for providers, insurers and patients nationwide as this was not "just" a data breach. It had a real impact on critical health infrastructure. It stopped payments and medication processing, forcing manual workarounds and emergency funding. The numbers that were confirmed in 2025 made the breach the largest healthcare data compromise ever, affecting almost 2/3rds of the U.S. population.

g) Jaguar Land Rover Supply Chain Attack

In August 2025, Jaguar Land Rover suffered what is widely regarded as the most economically damaging cyber incident in UK history. According to the Cyber Monitoring Centre, the attack is expected to cost £1.9 billion and brought production to a halt for five weeks. More than 5,000 businesses across JLR's global supply chain were affected, with full recovery not expected until January 2026.

The attack was attributed to the Scattered Lapsus$ Hunters, a loosely affiliated collective linked to groups such as Lapsus$, Scattered Spider, and ShinyHunters. By exploiting vulnerabilities in third-party supplier software, the attackers were able to move laterally into JLR's core systems. Ransomware crippled production and logistics networks, forcing temporary shutdowns at manufacturing sites in the UK, Slovakia, and Brazil. Beyond operational disruption, the attackers threatened to leak sensitive design and supplier data unless multi-million-pound ransom demands were met.

This incident showed how cyber-attacks on the supply chain can have immediate physical and economic consequences. It reinforced the need for stronger operational technology segmentation, secure software dependencies, and rigorous third-party assurance across industrial environments.

h) United Natural Foods Ransomware Attack

In June 2025, United Natural Foods, Inc. (UNFI), a leading food distribution company, demonstrated the real-world impact of cyberattacks on supply chains. UNFI, known as the primary distributor for Whole Foods and other grocers, detected unauthorized activity on its IT systems. To contain the threat, the company took affected systems offline, which temporarily crippled its ability to process orders and make deliveries. As a result, some grocery retailers experienced product shortages and delivery delays.

The disruption continued for multiple days, and UNFI stated that the incident would cause ongoing operational delays and additional costs. The food supply chain impact garnered attention from regulators. It highlighted the need for stronger cyber defenses in the distribution and manufacturing sectors, as even brief outages can have cascading effects on consumers.

i) Sepah Bank Cyber Attack

In June 2025, the hacktivist group Predatory Sparrow claimed responsibility for a cyber-attack on Bank Sepah, a major state-owned Iranian bank linked to the military. The bank's website, ATMs, and online banking services went offline, and branches closed, blocking customers from accessing accounts or making transactions. According to media reports, the attackers said they "destroyed data" as retaliation against the bank's alleged financing of illicit regime activities. The cyberattack on Bank Sepah's infrastructure underscored how adversaries increasingly use cyber warfare to target critical financial systems, severely disrupting civilian access to banking services.

3. High Impact CVEs Behind Major Breaches

Many of today's biggest security incidents did not begin with advanced attacks, but with well-known, exploitable flaws left unaddressed. The following high-impact CVEs opened the door to major breaches, highlighting just how critical rapid patching and proactive vulnerability management truly are.

a) CVE-2025-54236 – Adobe ColdFusion

Adobe Commerce and Magento Open Source were hit by a critical vulnerability, tracked as **CVE-2025-54236**, with a high severity score of 9.1. The flaw stems from improper input validation in the platform's REST API, allowing attackers to hijack customer sessions and take over user accounts without proper authentication. Soon after Adobe released the patch, researchers observed large-scale exploitation attempts, with hundreds of attacks recorded within a short span. Security teams found a significant number of online stores unpatched, making them easy targets for attackers. Successful exploitation can lead to unauthorized access to customer data, financial fraud, and the deployment of persistent backdoors. The incident highlights the urgent need for rapid patching in e-commerce environments, where delayed updates can directly impact customer trust, business continuity, and revenue.

b) CIVN-2025–0163 High-Risk Apple OS Vulnerabilities

Multiple high-severity vulnerabilities have been discovered across Apple operating systems, including iOS, iPadOS, macOS, watchOS, tvOS, and visionOS. These flaws originate from memory corruption issues, logic errors, improper input validation, and weak privilege controls. If exploited, attackers could gain unauthorized access, execute arbitrary code, steal sensitive data, bypass built-in security protections, or cause system crashes. Both personal users and enterprise environments are at risk, especially on unpatched devices.

c) CVE-2025-10035 – Fortra GoAnywhere MFT

A critical deserialization flaw in GoAnywhere MFT's License Servlet (affecting versions ≤ 7.8.3) allows an attacker, with a forged license-response signature, to inject malicious data, triggering arbitrary command execution and full remote code execution. A threat actor group tracked as Storm-1175 has already exploited this vulnerability since early September 2025, deploying remote-management tools, backdoors, and in some cases, ransomware payloads such as Medusa. Rated with a CVSS score of 10.0, the issue highlights the urgent need for organizations to immediately patch vulnerable instances and strengthen their defenses to prevent active exploitation.

4. The Evolution of Cyber Threats in 2025

In 2025, we saw significant development in the evolution of cyber threats, ranging from ransomware, hacktivism, rising mobile threats to the wide use of AI by the bad actors. New cyber threats were born with sophisticated attack methodologies. Based on the findings of different cybersecurity research, the most dominating threats that we have seen in 2025 are described below:

a) Social Engineering

In 2025, social engineering remains one of the most dominant cyber threats. Attackers exploit human trust at scale, making social engineering faster, more convincing, and more difficult to detect than ever before. For many years, phishing emails were used as the primary social engineering vector, and organisations became increasingly aware of these threats.

However, in 2025, social engineering expanded beyond traditional email-based campaigns, adopting multi-platform, cross-channel, and highly targeted approaches that leverage phone calls, messaging applications, and real-time impersonation. At the same time, attackers have evolved how email and browser-based social engineering attacks are executed, shifting toward interaction-driven techniques such as ClickFix and its variants. These methods guide users through seemingly legitimate workflows designed to bypass security controls and inadvertently execute malware.

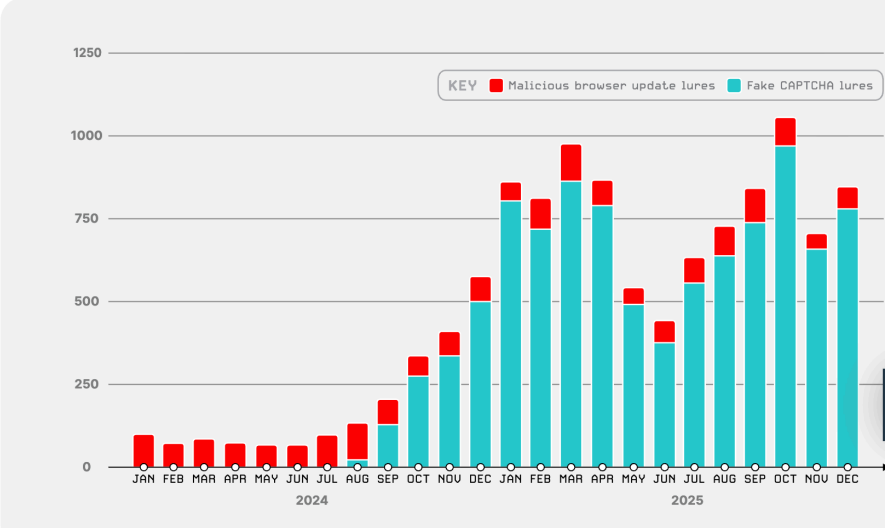
As per CheckPoint, ClickFix emerged as one of the most significant social engineering techniques in 2025. First observed in 2024, ClickFix is an initial access method in which attackers manipulate users into executing malicious actions by presenting them with fraudulent instructions. These instructions, typically delivered through compromised or attacker-controlled websites, malvertising, or brand-impersonation emails, are crafted to resemble routine verification steps such as CAPTCHAs, validation checks, or error fixes. By appearing as legitimate steps required to continue normal activity, users are manipulated into running attacker-controlled content that ultimately delivers malware.

In 2025, ClickFix activity increased by approximately 500% compared to the previous year and was observed in nearly half of all documented malware campaigns.

b) Malware

Malware continued to pose a persistent cybersecurity threat in 2025, affecting both individuals and organisations worldwide. Cybercriminals increasingly used malicious software to compromise systems, steal sensitive information, and gain unauthorised access to devices and networks. The spread of malware was often facilitated through phishing campaigns, malicious downloads, and compromised websites, highlighting the importance of maintaining strong cybersecurity practices and updated security systems.

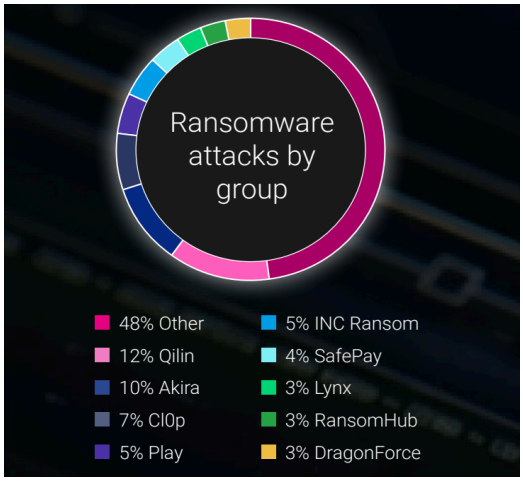
In 2025, Crowdstrike Intelligence observed that many cybercriminals have shifted from malicious browser update-related lures to fake CAPTCHA lures to entice victims to download and execute malware. The figure below highlights adversaries' rapid adoption and persistent use of fake CAPTCHA lures (compared to malicious browser update lures) over the past two years. In comparison to 2024, CrowdStrike Intelligence observed a 563% increase in incidents using fake CAPTCHA lures in 2025.



Source: CrowdStrike 2026 Global Cyber Threat Report

c) Ransomware

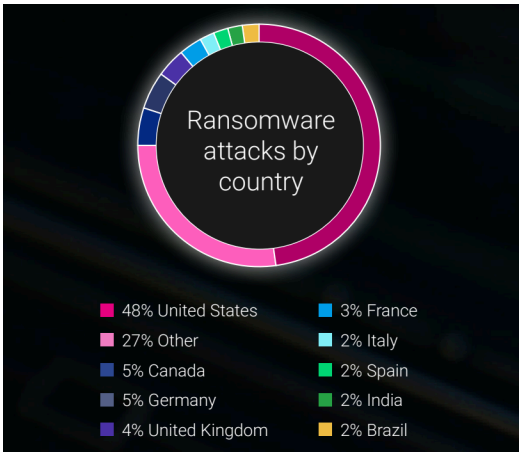
In 2025, ransomware remained the most disruptive and economically damaging form of cyber threat worldwide. While cybercrime continued to diversify across phishing, infostealers, supply-chain compromises, and AI-enabled attacks, ransomware distinguished itself by its scale, sophistication, and systemic impact on governments, critical infrastructure, and private enterprises. No longer limited to opportunistic encryption of files, ransomware operations evolved into highly organised, service-based criminal enterprises that combined data theft, extortion, reputational coercion, and in some cases operational sabotage.



The ransomware ecosystem in 2025 was characterised by professionalisation and fragmentation. Dozens of active ransomware groups operated under Ransomware-as-a-Service (RaaS) models, lowering the barrier to entry for affiliates while increasing attack volume globally. Campaigns became faster, more targeted, and increasingly data-driven, leveraging initial access brokers, credential harvesting, and AI-assisted social engineering to penetrate networks with greater efficiency.

At the same time, the economic dynamics of ransomware shifted. While reported incidents surged year-on-year, aggregate ransom payments showed signs of fluctuation as organizations strengthened backup strategies, improved detection capabilities, and benefited from coordinated law-enforcement disruptions. Nevertheless, average ransom demands rose significantly, reflecting attackers' focus on high-value targets and business disruption rather than merely data encryption.

The following section outlines the dominant ransomware groups and the countries most affected during the year.



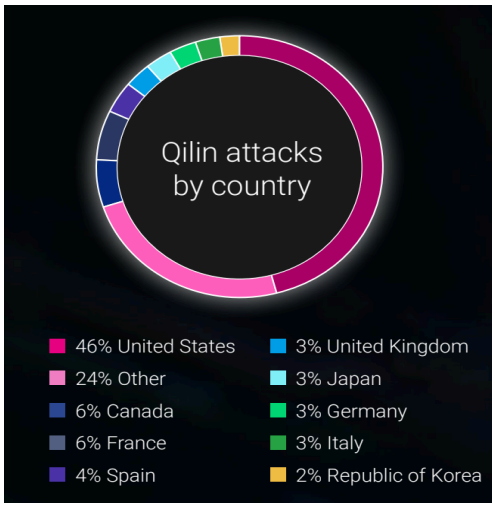
Most affected Country by Ransomware

The United States remained the most attacked country in the world by a large margin, accounting for almost half of all known ransomware events in 2025. Other attacks were heavily concentrated in Western Europe and other countries such as Brazil.

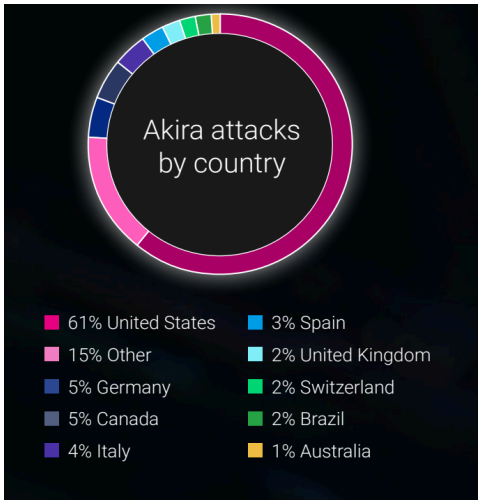
Ransomware Groups

In recent years, the expansion of ransomware has been fuelled by a consistent rise in the number of active groups. While many of these threat actors are relatively small groups - launching only a handful of attacks each month - their cumulative impact has steadily intensified. Although a few highly groups continue to account for a significant proportion of victims, the period when a single dominant brand such as LockBit or Conti could shape the entire ransomware ecosystem has effectively ended.

Sustained law-enforcement operations, arrests, infrastructure disruptions, and internal fractures have dismantled major operations and prompted affiliates to shift between different ransomware programs. Concurrently, the growth of ransomware-as-a-service (RaaS) models has lowered entry barriers, encouraging the emergence of smaller, agile, and often regionally focused groups that frequently rebrand and adapt. As a result, the ransomware landscape in 2025 appears structurally persistent yet increasingly fragmented, decentralised, and unpredictable.



In 2025, Qilin became the most active ransomware group of 2025, carrying out more attacks than any other two groups combined. Its rise suggests a mature affiliate model, strengthened by the collapse or fragmentation of LockBit, ALPHV, and RansomHub. Qilin targets mid-sized companies, regional firms, and local service providers across manufacturing, business services, healthcare, construction, and technology rather than large multinationals.



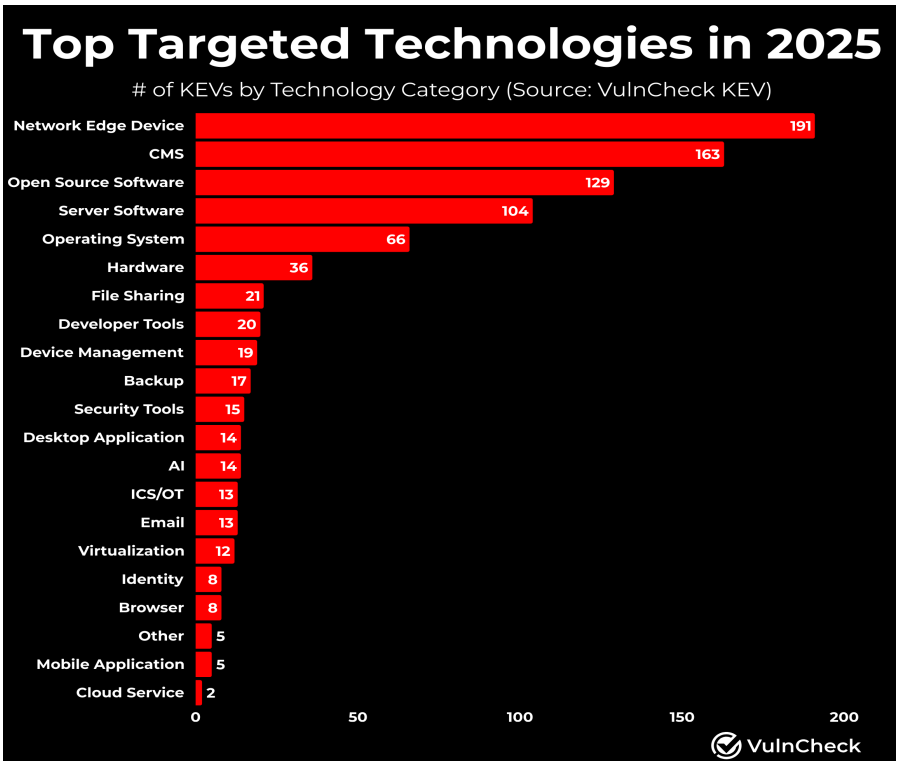
Akira was the second most active ransomware group in 2025 with activity concentrated in the United States, Germany, Canada, and Italy. The target groups of Akira are small and mid-sized organisations, including regional service providers, mid-market manufacturers, local public sector entities, and modest technology firms.

Source: Malware Report 2026

d) Vulnerabilities in Systems and Applications

The year 2025 stood out for the number of severe zero-day vulnerabilities, in which attackers compromised systems before the vulnerabilities were publicly disclosed and retained access even after patches were applied. During the year, attackers continued to exploit vulnerabilities known for years that remained unpatched. Increasingly, and with greater specificity, attention has focused on state-backed groups that search for and exploit vulnerabilities in critical infrastructure systems.

According to VulnCheck, more than 48,000 vulnerabilities were reported in 2025, an increase of around 20% from 2024. Serious vulnerabilities were found in network devices, industrial automation systems, operating systems and a wide range of other software. The statistics gathered from VulnCheck indicates that network edge devices such as firewalls, VPNs, and proxies were mostly targeted in 2025. These Internet-facing devices often serve as a jumping-off point into an enterprise environment or home network. Content management systems, largely dominated by the WordPress ecosystem, are also frequent targets because they are commonly exposed to the internet. Open source software ranked third in 2025, followed by server software and operating systems such as Microsoft Windows, Linux, Apple, and Android.

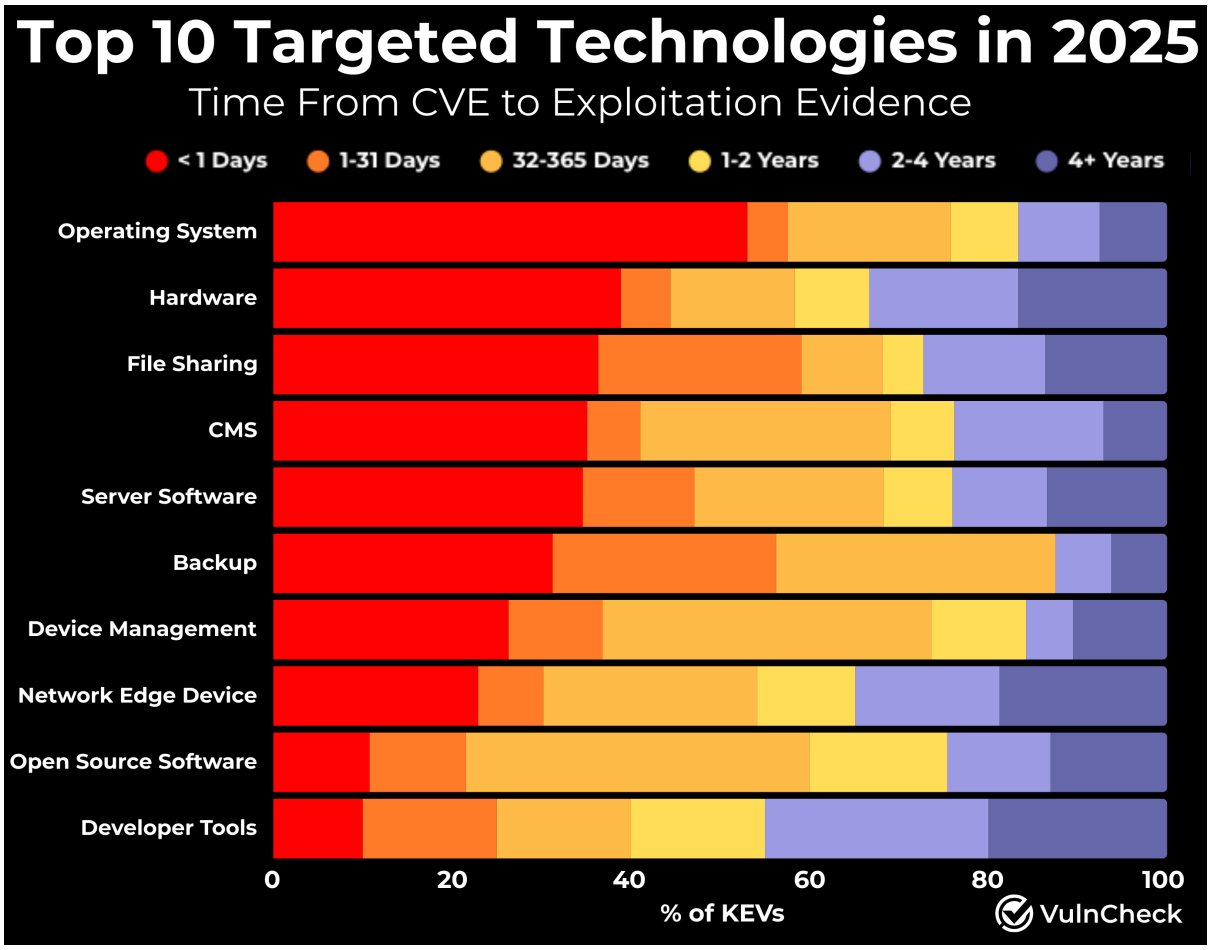


Source: VulnCheck

However, exploitation spans a broad range of enterprise technologies and extends beyond these categories to include hardware devices, most often camera systems, as well as file sharing platforms, developer tools, device management systems, backup solutions, security tools, desktop applications, AI systems, ICS and OT environments, email platforms, virtualisation technologies, identity systems, browsers, mobile applications, cloud services, and

more. Threat actors are opportunistic, leveraging both older, well-known vulnerabilities and newly disclosed flaws to access systems and establish footholds across the enterprise.

Apart from the top targeted technologies, there is also important to highlight the vulnerability exploitation timeline relative to the CVE issuance. This provides additional insight into the relationship between exploitation and disclosure. For 2025, Operating Systems were mostly exploited because vendors such as Microsoft, Apple, and Android frequently disclose evidence of exploitation alongside their security advisories. In the second position, there is hardware which is mostly targeted. In this category, these were vulnerabilities camera systems. This likely reflects the relative immaturity of vulnerability disclosure and issuance practices among hardware manufacturers. While each category could warrant its own dedicated research project, this analysis provides defenders with a clearer sense of how quickly they need to prioritize patching for each technology.



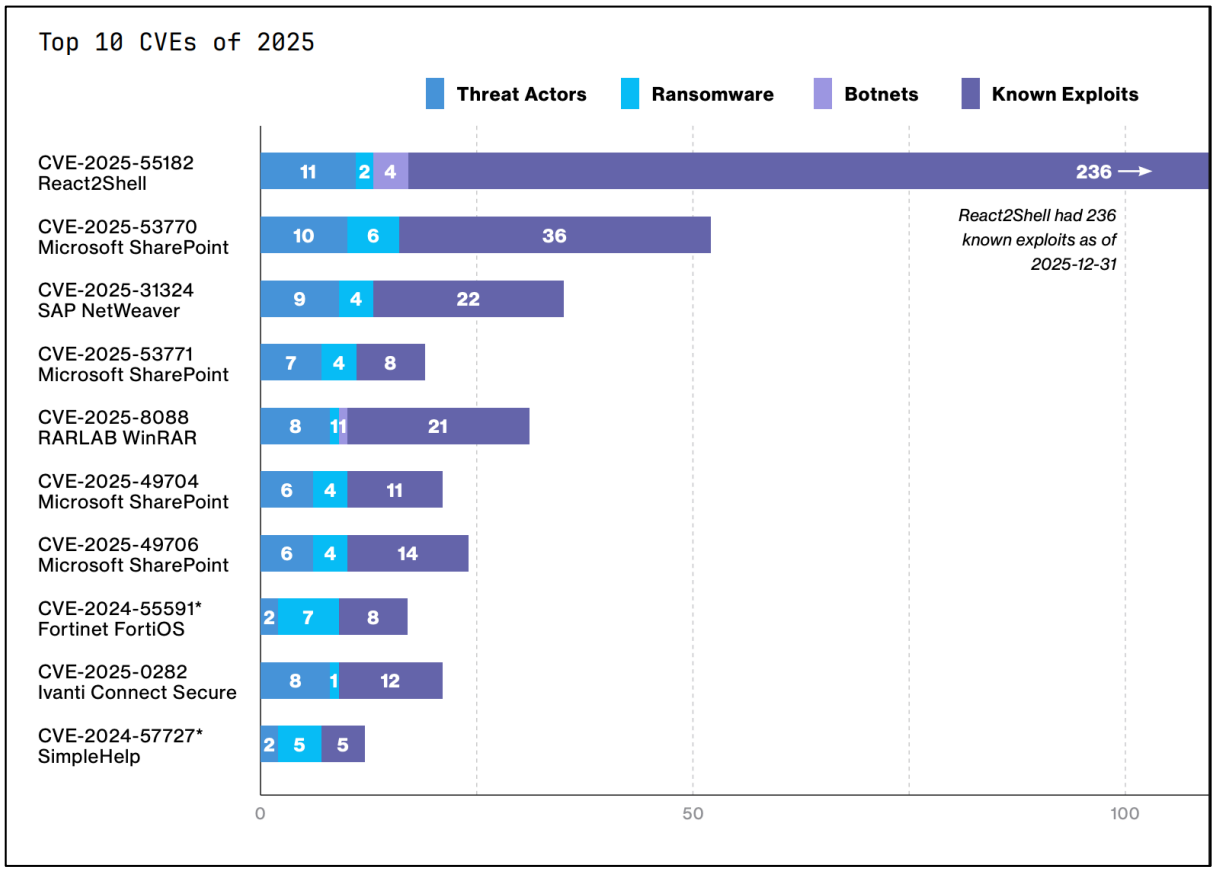
Source: VulnCheck

Top CVEs 2025 - Routinely Targeted Vulnerabilities (RTVs)

Every year, there is a subset of vulnerabilities that are widely exploited by attackers because they are particularly valuable initial access vectors, trivially exploitable and internet-accessible. Many RTVs score highly across multiple key areas, with the top targeted CVEs of 2025 accumulating both a wide variety of threat activity and deep public exploit benches. It's

abundantly clear from the data that certain vulnerabilities stand well above the rest in terms of attention and impact.

In 2025, CVE-2025-55182, a remote code execution (RCE) flaw in React Server components tops the list with 236 valid public exploits. By December 31, "React2Shell" had amassed more public exploits than any other vulnerability in history, surpassing the long-reigning "pwnkit" flaw (CVE-2021-4034, a Linux local privilege escalation) as the industry's most publicly researched CVE.



Source: VulnCheck, 2026

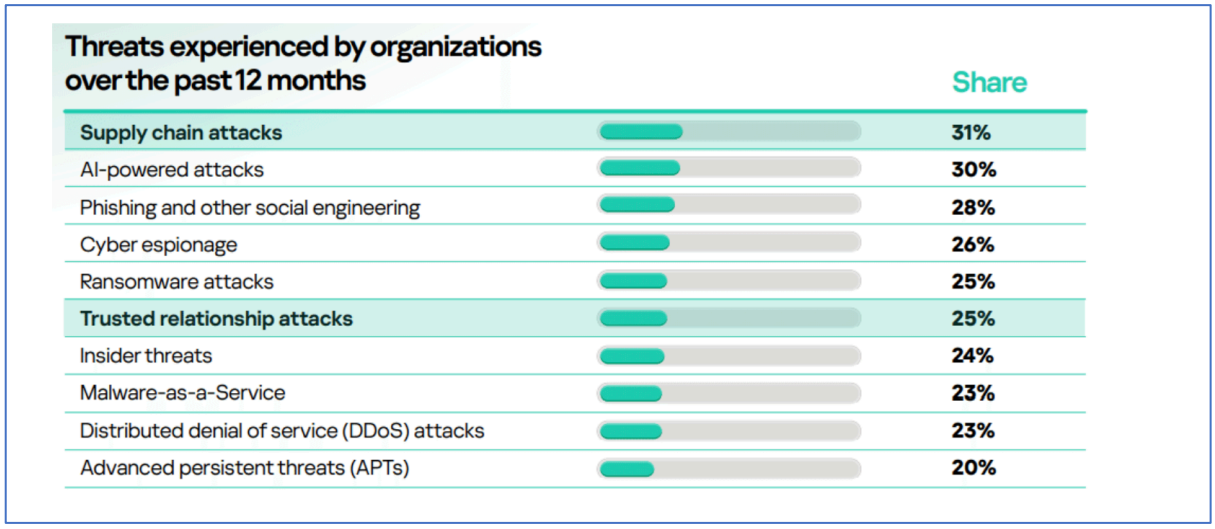
e) Supply Chain Attacks

Supply chain attacks have emerged as the most common cyberthreat facing businesses over the past year, a new Kaspersky global study shows. The findings reveal that nearly every third company had to confront a supply chain threat over the past year, with supply chain risk exposure exceeding the global average in Mexico (43%), China (40%) and Spain (40%).

According to recent data from the World Economic Forum, nearly two thirds (65%) of large enterprises indicate third-party and supply chain vulnerabilities as their greatest barriers to cyber resilience in today's interconnected digital landscape. To evaluate organisations' vulnerability to this threat, Kaspersky's internal market research center commissioned a global study, examining how these risks are evolving and the extent to which businesses around the world are being exposed.

According to the Kaspersky-commissioned survey, 31% of enterprise businesses had been impacted by a supply chain attack in the course of the past 12 months, which is more than any other type of cyberthreat. The supply chain threat is acutely focused on the most connected organisations, with large enterprises reporting the highest rate of experienced attacks - 36% - compared to counterparts from low and mid-size enterprise.

Moreover, the statistics reveal that over the past year, trusted relationship attacks ranked in the Top 5 most common threats, having affected a quarter (25%) of companies globally. Most frequently attacks abusing existing connections between organizations were suffered by organizations in Turkey (35%), Singapore (33%) and Mexico (31%).



Source: Kaspersky

f) Artificial Intelligence Related Threats

In 2025, Artificial intelligence (AI) was so deeply embedded in cyber activity that distinguishing "AI-related attacks" from general digital operations became increasingly challenging. In contrast to 2023–2024, when attackers' use of AI was easily recognisable, in 2025 AI use became so commonplace that it faded into the background of attack operations. Throughout 2025, threat actors not only refined and expanded their use of AI but also increasingly attempted to target the AI ecosystem itself. As enterprises adopt agentic frameworks, MCP servers, and locally deployed models, these environments have become the new attack surfaces.

Deepfakes

2025 saw an escalating series of warnings from regulators, financial institutions, law-enforcement agencies, and industry bodies highlighting deepfakes as an active and rapidly growing threat to businesses. In July, OpenAI CEO Sam Altman added urgency to these concerns, stating that generative AI had already "fully defeated" the face and voice authentication systems used by banks and was creating "a significant impending fraud crisis."

A 2025 analysis by IBM found that AI played a role in 16% of breaches with deepfake voice or video manipulation accounting for 35% of those incidents. Several high-profile fraud cases demonstrated that criminals can now create impersonations convincing enough to succeed in live video calls.

Deepfake voice, image, and video impersonation now requires minimal expertise and only a handful of reference images or seconds of audio. Criminals are using these capabilities across a wide spectrum of attacks: creating fabricated IDs for financial fraud; mimicking IT or helpdesk staff to persuade employees to share passwords, reset multi-factor authentication (MFA), or approve remote access; and impersonating executives to conduct highly convincing forms of CEO fraud.

Autonomous ransomware

One of the most significant cybersecurity developments of 2025 was the first in-the-wild use of autonomous AI agents to scale extortion operations. Historically, the biggest global ransomware groups struggled to scale beyond a few hundred attacks per month, limited by the need for skilled operators performing hands-on-keyboard intrusions.

g) Internet of Things (IoT) Attacks

The volume of IoT-focused cyberattacks continues to increase. Security analysts report a "staggering" level of background noise from automated threats. In 2025, an average of 820,000 IoT hacking attempts occurred each day. Notably, global threat data showed a 16.7% rise in active scanning activity worldwide, as attackers' bots relentlessly probe for open ports, default passwords, and unpatched gadgets. This always-on probing means virtually every internet-connected device is tested by attackers, often within minutes of going online.

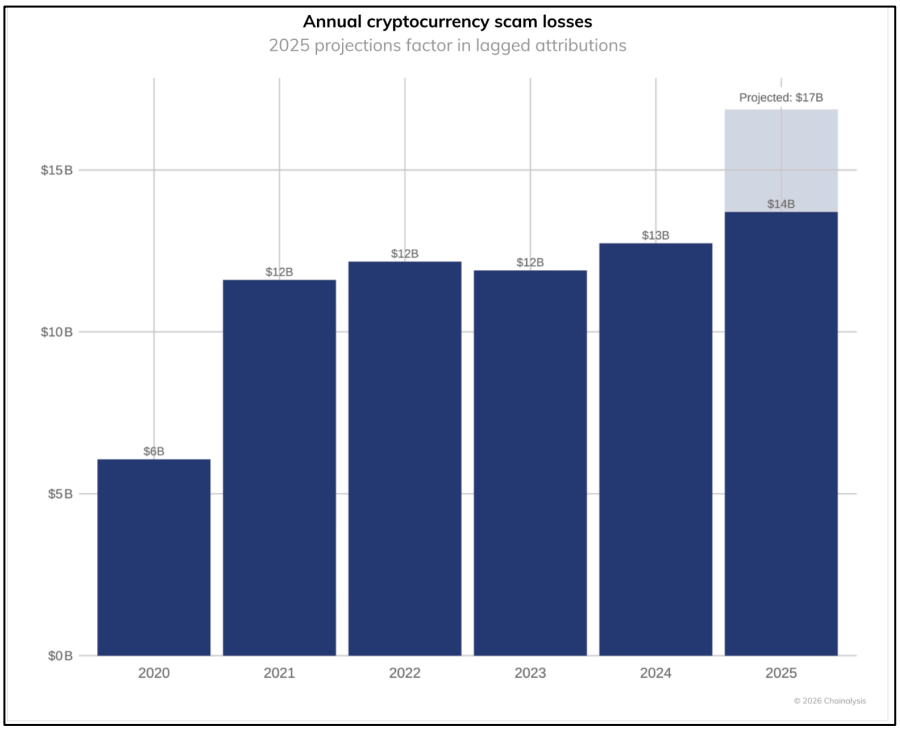
According to Zscaler's mid-2025 ThreatLabz report, routers accounted for over 75% of all observed IoT cyberattacks. This is because routers are ubiquitous, often poorly secured, and sit at key network choke points. Attackers exploit a litany of router vulnerabilities to execute malicious code and take control, frequently using command injection or buffer overflow flaws to gain a foothold. Once hijacked, a router can be weaponized to funnel traffic (becoming part of a DDoS botnet) or to snoop on and redirect data in man-in-the-middle attacks. Notably, researchers have flagged certain brands/models – for example, older Netgear routers are frequent targets – where unpatched firmware allows remote code execution (e.g., exploits like CVE-2016-10174 and CVE-2018-10561 are still seen in the wild).

h) Scams and Fraud

As per Chainalysis Report, in 2025, cryptocurrency scams received at least $14 billion on-chain, which represent a significant increase from the $9.9 billion that were reported in 2024. This year's data show that scammers continue to adapt and innovate, with the average scam payment increasing from $782 in 2024 to $2,764 in 2025, a growth of 253% YoY. Overall scam

inflows have also surged, particularly through impersonation tactics that saw a staggering 1400% year-over-year (YoY) growth.

While high-yield investment programs (HYIP) remain dominant categories by volume, there is an increasing convergence across scam types as fraudsters leverage AI, sophisticated SMS phishing services, and complex money laundering networks to target victims more effectively than ever before. Traditional scam categorizations are becoming less distinct as fraudsters incorporate multiple tactics into their operations.

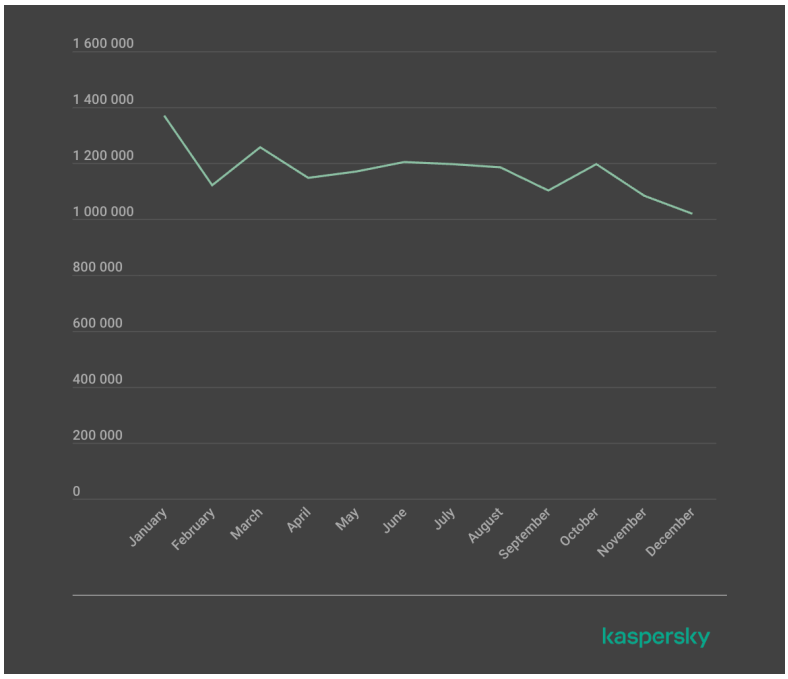


Source: Chainalysis

i) Mobile Threats

In 2025, the mobile threat landscape continued to expand significantly, with attackers exploiting vulnerabilities in mobile operating systems, malicious applications, and social engineering techniques to compromise devices and steal sensitive information. The rapid adoption of mobile banking and digital wallet services has further incentivised financially motivated cybercrime, leading to a surge in mobile malware, phishing campaigns, and banking Trojans targeting smartphone users. Consequently, mobile platforms have emerged as a critical attack vector within the broader cybersecurity threat landscape.

As per Kaspersky, in 2025, cybercriminals launched an average of approximately 1.17 million attacks per month against mobile devices using malicious, advertising, or unwanted software. In total, Kaspersky solutions blocked 14,059,465 attacks throughout the year.



Source: SecureList

Moreover, a significant increase was noted in specific threats – most notably mobile banking Trojans and spyware – even though adware remained the most frequently detected threat overall. As per Kaspersky, the number of new banking Trojan installation packages rose to 255,090, representing a several-fold increase over previous years. Among the mobile threats detected, an increased prevalence was seen in preinstalled backdoors, such as Triada and Keenadu. Certain mobile malware families continue to proliferate via official app stores.

j) Cloud Based Attacks

In 2025, cloud security continued to be a growing concern as organisations increasingly adopted cloud-based services to support digital transformation and remote operations. According to AppSecure Cloud Security Statistics 2025, around 54% of organizations reported an increase in attacks targeting cloud infrastructure in 2025, highlighting the growing attractiveness of cloud environments for cybercriminals. Moreover, approximately 27% of organizations experienced a security breach involving their public cloud infrastructure. While cloud technologies offer flexibility and scalability, they also introduce new security challenges, including misconfigurations, unauthorised access, and data exposure. As a result, strengthening cloud security practices and implementing proper access controls became essential to protecting sensitive data and ensuring the resilience of digital services.

5. Useful Statistics: Cyber Security in 2025

Cybercrime Cost
Cybercrime costs are expected to escalate worldwide to almost $14 trillion by 2028[1].

Ransomware - Downtime
Businesses are paying $53,000 per hour, on average, due to downtime caused by ransomware. [2]

AI Cyber Attacks
59% of businesses experienced a successful attack in the past 12 months - and 33.5% believe AI was involved.[3]

Malware Attacks
Around 27% of all malware attacks right now involve ransomware [4].

Phishing
60% of recipients fall victim to GenAI-driven phishing attacks, comparable to traditional attack numbers. [5]

Spear Phishing
Up to 74% of attacks involve spear phishing.[6]

Insider Threats
74% of companies claim insider threats are becoming more frequent. [7]

Human Element
95% of all data breaches involve some kind of human element or error. [8]

Cloud Security
27% of business operators experience public cloud security issues, with 23% of them alone caused by misconfigurations.[9]

Denial of Service
DDoS (Distributed Denial of Service) attacks are increasing by 20% year-on-year. [10]

Data Breach
On average, cross-industry, it takes companies 204 days to spot a data breach and 73 days to contain it. [11]

Business Email Compromise
Business Email Compromise or BEC attacks are costing companies an average of $4.67 million per attack and account for 8.5% of all data breaches. [12]

Source:

1. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
2. https://www.pentestpeople.com/blog-posts/ransomware-2022-facts-and-statistics
3. https://www.vikingcloud.com/resources/the-2025-cyber-threat-landscape-report-cyber-risks-opportunities-resilience
4. https://www.getastra.com/blog/security-audit/ransomware-attack-statistics/
5. https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
6. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish
7. https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurucul/
8. https://www.infosecurity-magazine.com/news/data-breaches-human-error/
9. https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/
10. https://blog.cloudflare.com/ddos-threat-report-for-2024-q2/
11. https://secureframe.com/blog/data-breach-statistics
12. https://media.trustradius.com/product-downloadables/L2/IL/A7IHG9ZZJ5XP.pdf

6. Cyber Threat Trends - Mauritius

Mauritius has witnessed a steady increase in cyber incidents in recent years, largely driven by the growing adoption of digital technologies across government services, businesses and the general public. As more citizens rely on online platforms for banking, communication, e-commerce and administrative services, cybercriminals are increasingly targeting Mauritian users through a variety of methods such as phishing emails, online scams, social engineering schemes, malicious links and the compromise of social media and messaging accounts. Financially motivated cybercrime remains one of the most prevalent threats, with fraudsters attempting to deceive victims into disclosing sensitive information or transferring funds. In parallel, emerging threats such as ransomware, malicious mobile applications and data breaches continue to pose risks to organisations and individuals alike.

In this evolving threat environment, the Computer Emergency Response Team of Mauritius (CERT-MU) plays a key role in monitoring cyber threats and coordinating the response to cybersecurity incidents at the national level. CERT-MU receives and analyses incident reports from individuals, organisations and critical sectors, and provides technical guidance and support to mitigate cyber incidents. In 2025, CERT-MU responded to more than 5000 incidents, including cases of hacking, phishing, sextortion, and malware attacks. These incidents are primarily reported through the Mauritian Cybercrime Online Reporting System (MAUCORS), which serves as the national platform for reporting cybercrime and connects key institutions such as CERT-MU, the Cybercrime Unit of the Mauritius Police Force, the Data Protection Office, and the Information and Communication Technologies Authority

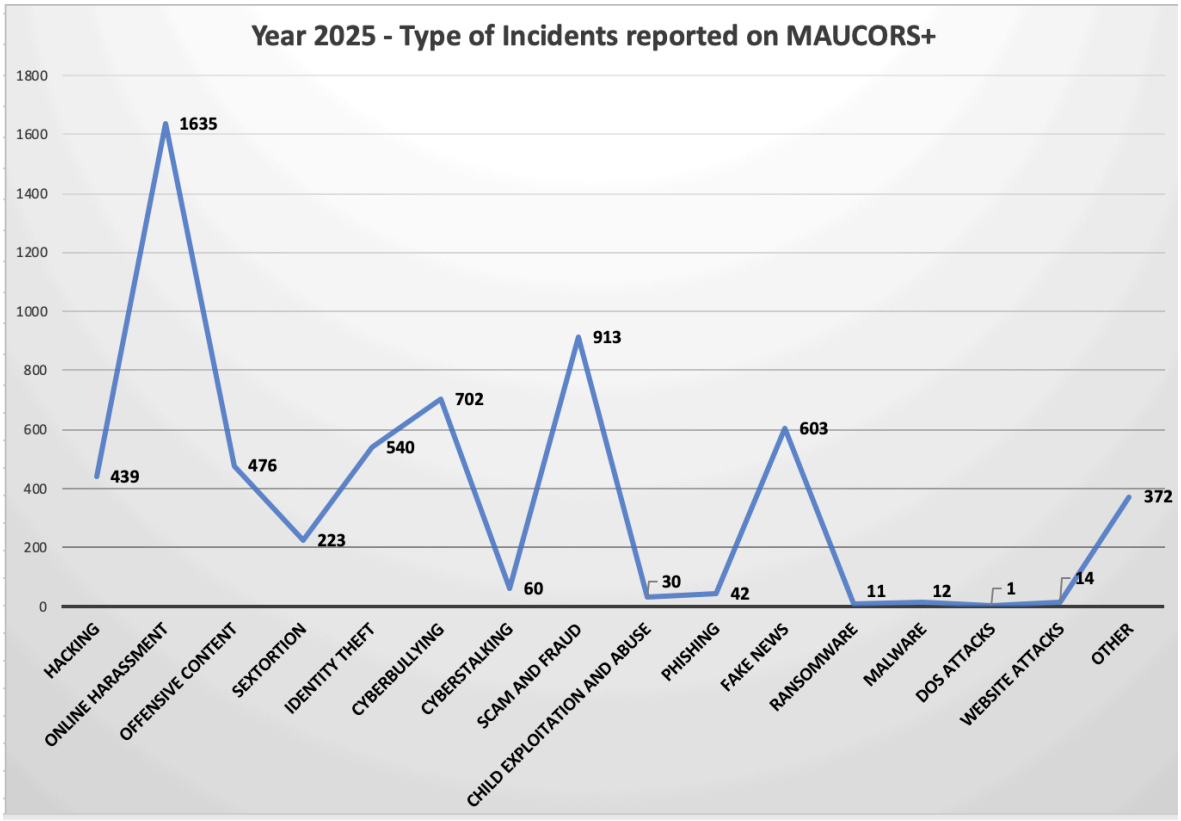
CERT-MU also carries out continuous awareness campaigns, capacity-building initiatives and collaboration with regional and international cybersecurity communities to strengthen the country's cyber resilience. The increasing number of reported incidents highlights the need for continued vigilance, stronger cybersecurity practices and greater public awareness in order to safeguard Mauritius' digital ecosystem.

7. Analysis of Cyber Incidents 2025

a) 2025 Overall Local Incident Trend

In 2025, 6073 incidents were reported on the Mauritian Cybercrime Online Reporting System (MAUCORS+), managed by CERT-MU. The analysis of incidents in 2025 provides an overview of the cyber threats affecting individuals in Mauritius. However, it should be noted that the number of reported incidents may not fully reflect the actual scale of cyber incidents occurring in the country. In many cases, victims may refrain from reporting incidents due to fear, embarrassment, reputational concerns, or a lack of awareness of the available reporting mechanisms. Consequently, the figures presented are likely to represent only a portion of the incidents experienced by the public.

Based on the data collected, a significant proportion of the incidents reported in 2025 are related to social media misuse and harmful online behaviour. The most frequently reported category was online harassment, highlighting the increasing misuse of digital platforms for intimidation, threats, and abusive conduct. This trend reflects the widespread use of social media platforms and messaging applications among the population.

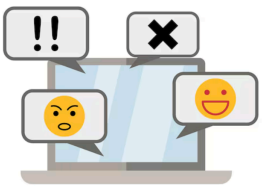


The key highlights are:

ONLINE HARASSMENT

1635 cases of online harassment were reported on the MAUCORS+ platform. These incidents involve abusive, threatening, or offensive behaviour directed at individuals through social media or messaging platforms. Such actions can have significant psychological and emotional impacts on victims and contribute to a hostile online environment.

Scam and fraud also represent a major category of reported incidents, with **913 incidents** recorded during the year. These incidents generally involve fraudulent schemes carried out through social media platforms, messaging applications, and online marketplaces, where cybercriminals attempt to deceive victims into transferring money or disclosing sensitive information.



CYBERBULLYING

702 cases of cyberbullying were reported in 2025. These incidents involve the use of digital platforms, particularly social media and messaging applications, to intimidate, harass, or humiliate individuals. Cyberbullying is particularly concerning among young internet users and can have serious emotional and psychological effects on victims.

.

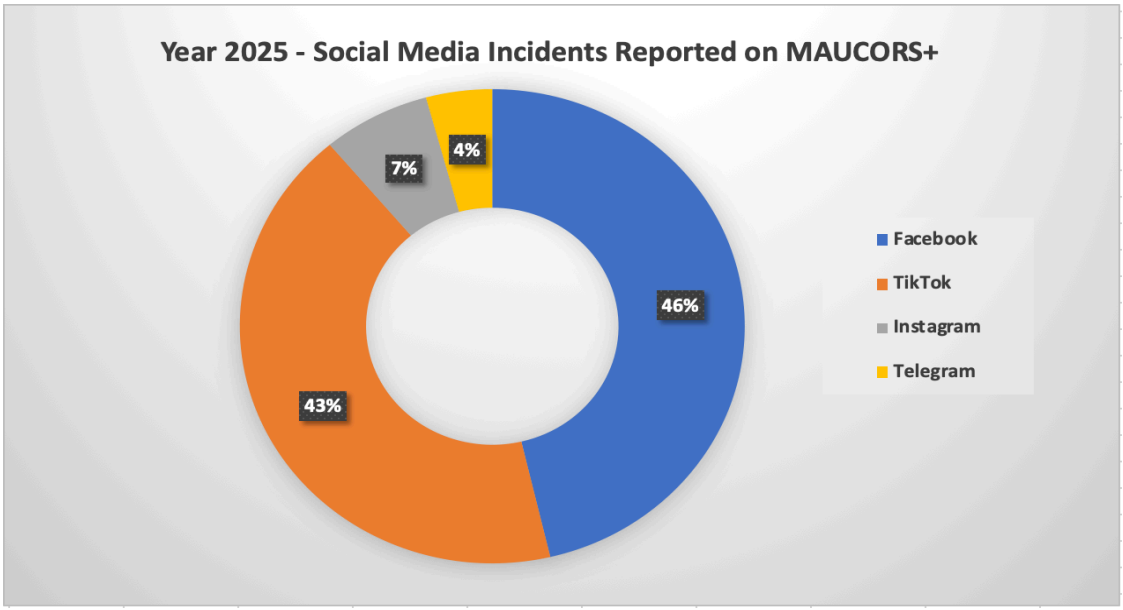
603 incidents of **fake news** were reported in 2025, which involved the circulation of false or misleading information through social media and messaging platforms, often designed to manipulate public perception or create confusion. The rapid spread of such content highlights the growing challenge of misinformation in the digital space.

540 cases of identity theft were reported in 2025. These incidents involve the unauthorised use of an individual's personal information or online identity to impersonate them on social media or other digital platforms. Such activities are often carried out to deceive others, conduct scams, or damage the reputation of the victim.

b) Social Media Incidents

In Mauritius, social media platforms such as Meta (Facebook), TikTok, Instagram and messaging applications like WhatsApp are widely used for communication and information sharing. However, these platforms are increasingly being exploited by cybercriminals. The increasing reliance of citizens on digital platforms for communication, commerce, and information sharing has expanded the potential attack surface for cybercriminals who exploit these environments to conduct various malicious activities.

As per the graph below, in 2025, the majority of incidents reported through MAUCORS+ were associated with the Facebook platform, accounting for 46% of cases. This can largely be attributed to Facebook's widespread usage in Mauritius and its integration with services such as Facebook Marketplace and Messenger, which are frequently exploited for scams, impersonation, fake profiles, and harassment.



TikTok accounted for 43% of reported incidents, reflecting the rapid growth of the platform, particularly among younger users. Many of the reported cases are linked to cyberbullying, offensive content, and misuse of personal videos or images, highlighting concerns related to online behaviour and digital safety.

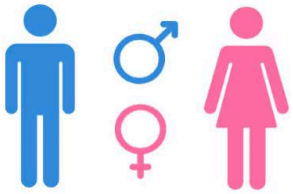
Instagram represented 7% of reported incidents, with cases often involving account compromise, impersonation, and harassment through direct messages or fake accounts. Although the proportion is lower, the platform remains a vector for identity misuse and social engineering attempts.

Finally, Telegram accounted for 4% of incidents, where cases are typically linked to the circulation of misleading information, scams, and the sharing of harmful or inappropriate content within groups or channels.

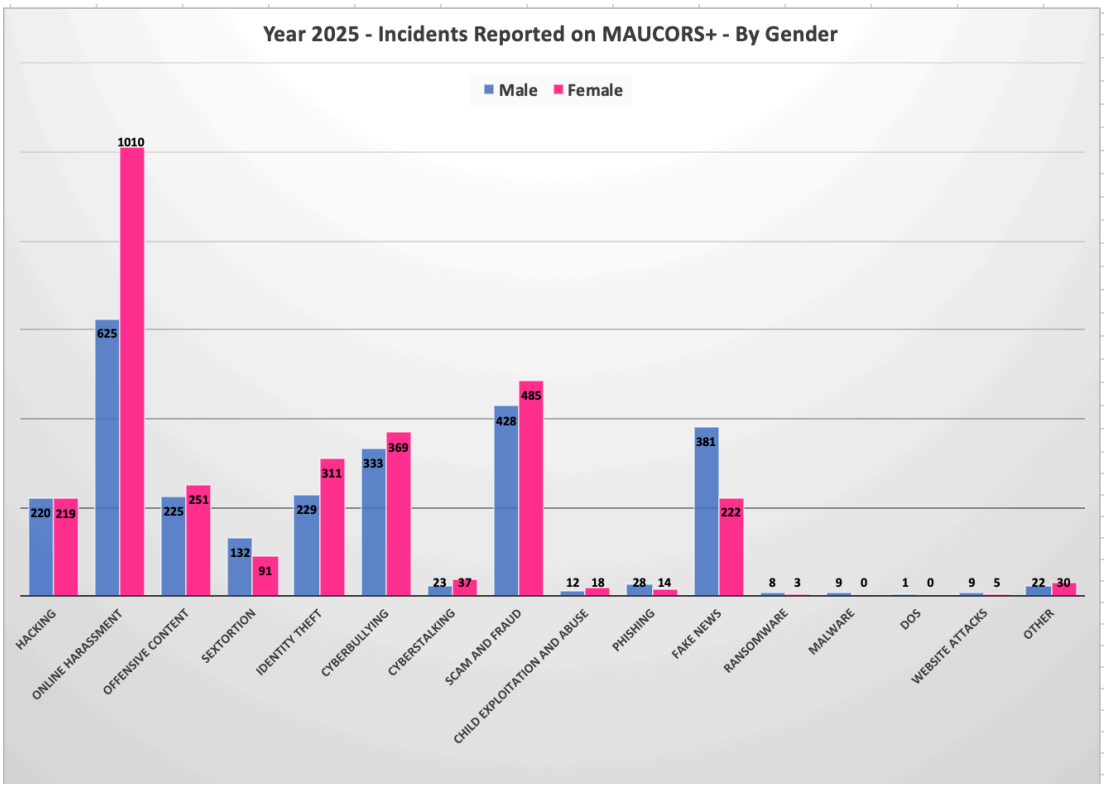
Overall, the analysis indicates that popular social media platforms continue to serve as key channels through which cyber incidents affecting the public are perpetrated, largely due to their high user engagement and the ease with which malicious actors can reach potential victims.

c) Gender Based Analysis of Incidents

In 2025, a total of 2,685 incidents were reported by men, while 3,065 incidents were reported by women through the MAUCORS+ platform. The gender-based analysis of incidents reported on the MAUCORS+ platform in 2025 indicates notable differences in the types of cyber incidents affecting male and female victims. Overall, the data shows that female users reported a higher number of incidents in several categories, particularly those linked to online harassment, scams, identity misuse, and cyberbullying. This highlights the greater exposure of women to certain forms of online abuse and social engineering attacks.



Incident Statistics	
Male: 2685	Female: 3065



The most significant disparity is observed in online harassment, where female victims account for a substantially higher number of cases compared to males. This suggests that women are more frequently targeted through abusive messages, intimidation, and offensive behaviour on social media platforms and messaging applications.

Similarly, scam and fraud incidents show a higher number of reports from female victims, indicating that cybercriminals are increasingly targeting women through deceptive schemes

such as fraudulent offers, impersonation, or financial scams conducted via social media and messaging platforms.

In the case of cyberbullying and identity theft, female victims also represent a larger proportion of the reported incidents. These cases often involve harassment, impersonation, or misuse of personal information, which can lead to reputational damage and emotional distress.

Conversely, certain categories show a higher number of reports from male victims. For instance, fake news incidents appear to affect male users more frequently, suggesting that men may be more involved in reporting cases related to misinformation or the circulation of misleading content online. Additionally, sextortion cases are reported more frequently by male victims, which reflect targeted extortion schemes commonly carried out through social media or online interactions.

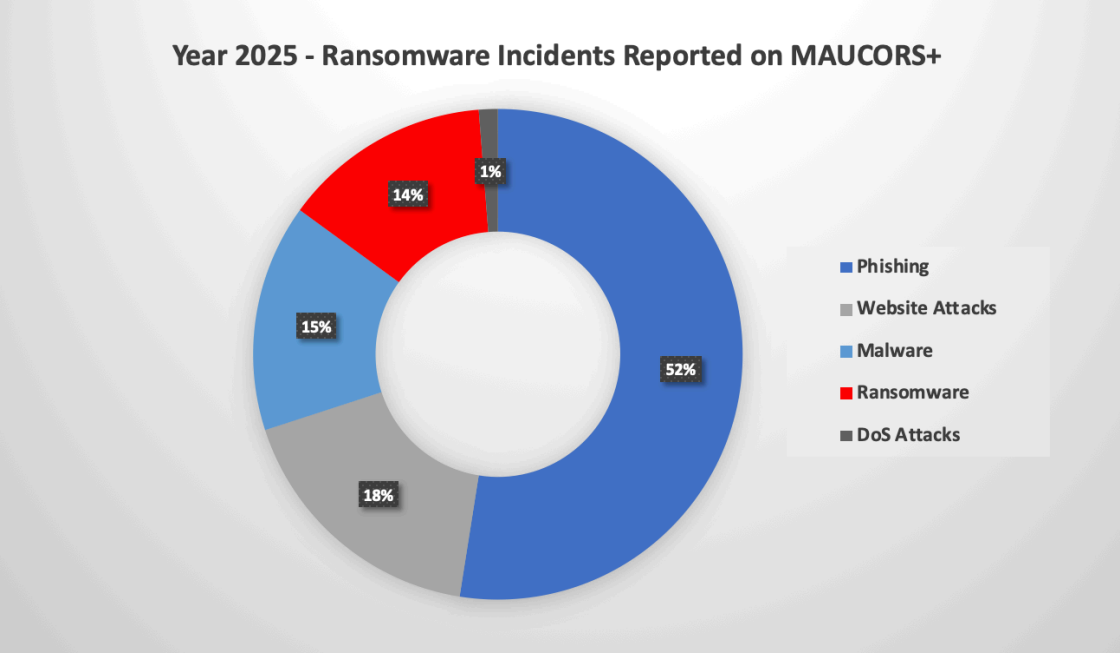
Overall, the analysis highlights that human-centric cyber threats, including harassment, fraud, and social engineering, continue to disproportionately affect certain groups, particularly women. These findings emphasise the importance of strengthening online safety awareness, digital literacy initiatives, and reporting mechanisms to better protect vulnerable users and address harmful online behaviour.

d) Technical Incidents

In addition to incidents related to social media misuse and online behaviour, a number of technical cyber incidents were also reported on the MAUCORS+ platform in 2025. These incidents typically involve malicious software, fraudulent attempts to obtain sensitive information, or attacks targeting websites and online systems. Although the number of reported cases in these categories remains relatively lower compared to human-centric threats such as scams and harassment, they continue to pose risks to individuals and organisations by compromising systems, disrupting services, and exposing sensitive data.

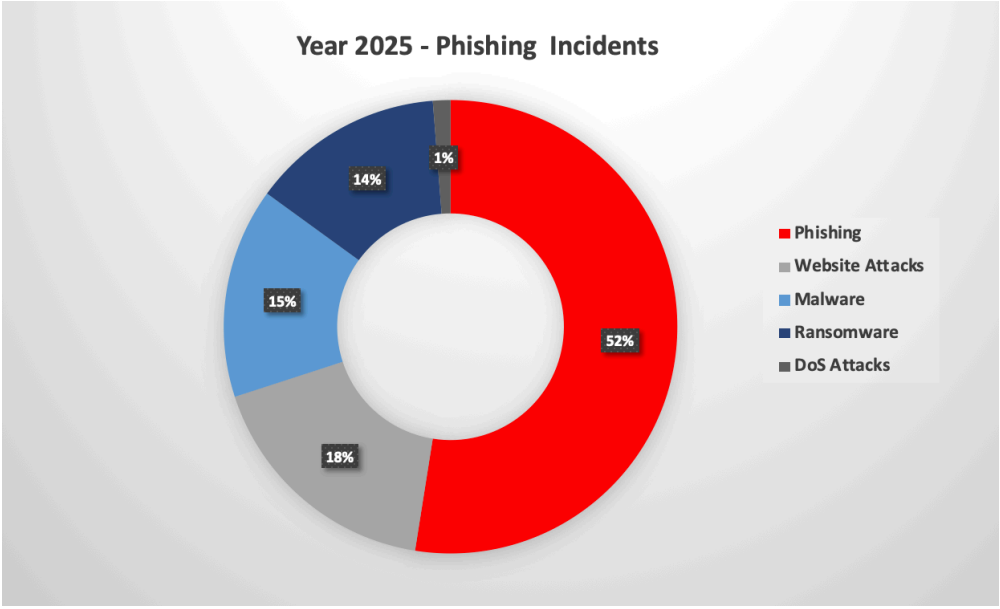
Ransomware

In 2025, 14% of incidents reported on MAUCORS+ platform was ransomware. It is also important to note that ransomware attacks are often underreported. This is because organisations choose to manage such incidents internally due to reputational or operational concerns. Despite the relatively low number of reported cases, there have been reports indicating that financial institutions and other organisations have been targeted by ransomware groups such as the Thegentlemen and Qilin groups. These developments highlight the continued risk posed by organised ransomware groups, which frequently target sectors handling sensitive data or financial transactions.



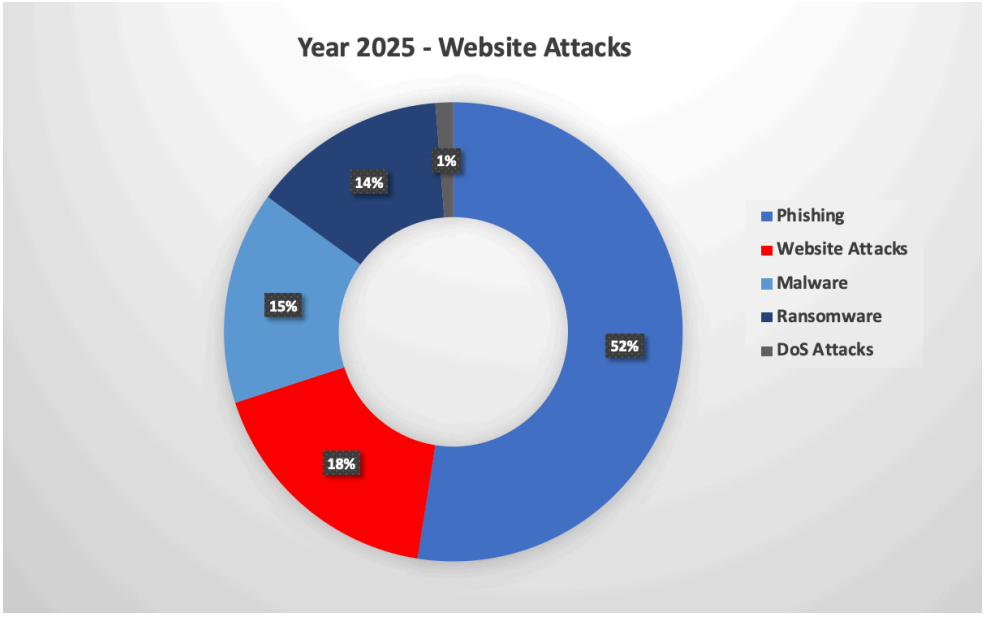
Phishing

In 2025, 42 phishing incidents were reported on the MAUCORS+ platform. Phishing remains one of the most commonly used techniques by cybercriminals to obtain sensitive information such as login credentials, personal data, and financial details. These attacks are typically carried out through fraudulent emails, SMS messages, or links circulated through social media and messaging applications, often impersonating trusted organisations such as banks, delivery services, government institutions, or well-known companies. In many cases, the messages create a sense of urgency, prompting victims to click on malicious links or provide confidential information. Although the number of reported cases appears relatively limited, phishing attempts are significantly underreported, as many users may not recognise such messages as malicious or may simply ignore them without reporting the incident.



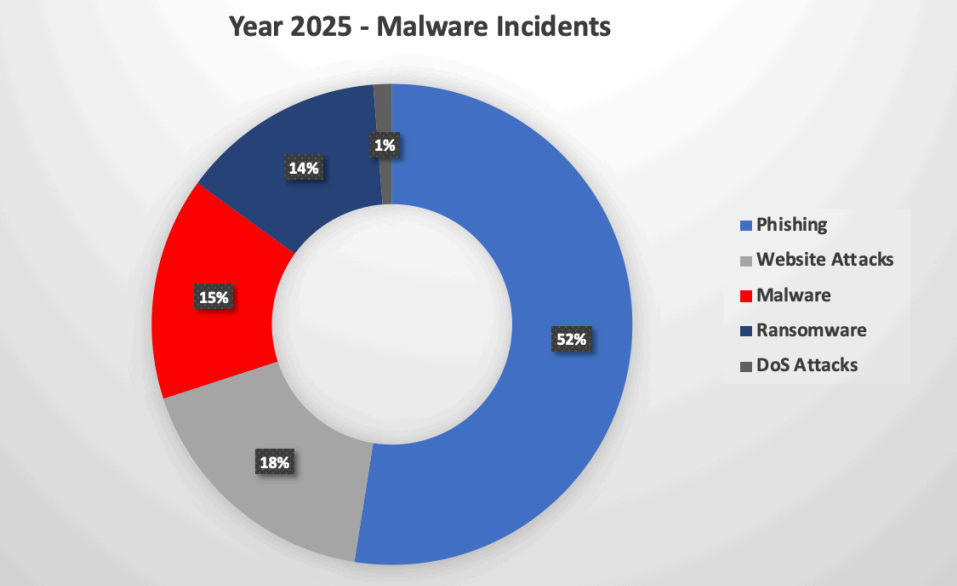
Website Attacks

In 2025, 18% of the technical incidents reported on the MAUCORS+ platform was related to website attacks. These incidents typically involve attempts by malicious actors to exploit vulnerabilities in web applications or servers in order to gain unauthorised access, deface websites, or disrupt online services. In some cases, attackers may also inject malicious code, redirect users to fraudulent websites, or attempt to extract sensitive information stored on the system. Such attacks can lead to service disruption, reputational damage, and potential exposure of confidential data if not properly mitigated. These incidents highlight the importance for organisations to regularly update their systems, conduct vulnerability assessments, and implement robust security controls to secure their online platforms.



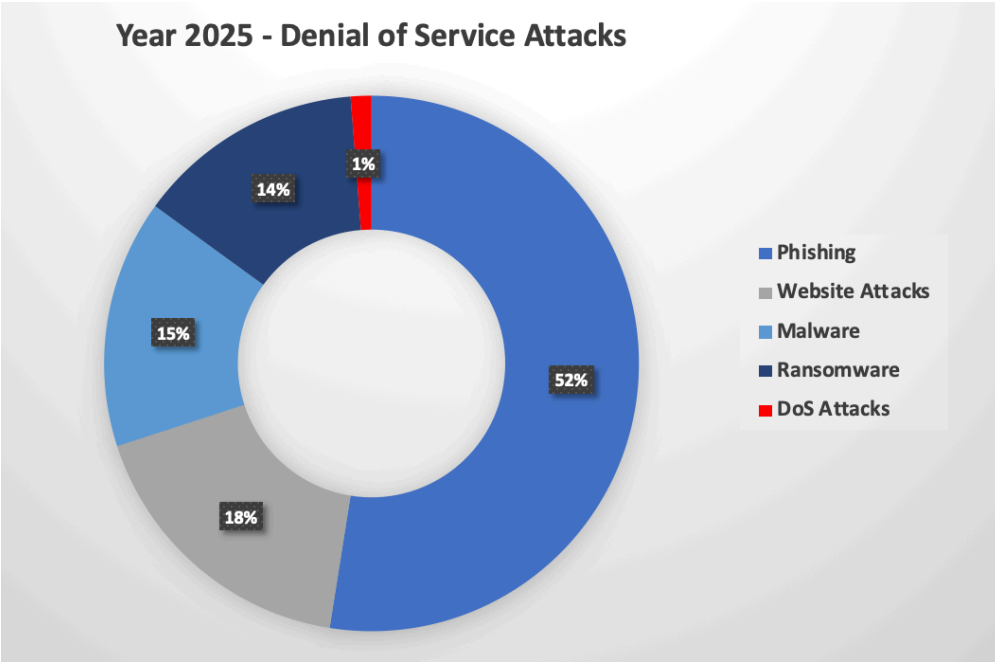
Malware

15% of the incidents reported were related to malware infections. The reported cases mainly involved devices becoming infected after users downloaded files or applications from untrusted sources, opened malicious email attachments, or accessed compromised websites. In several instances, the infections resulted in suspicious system behaviour such as unauthorised programs running in the background, redirection to unknown websites, or the exposure of personal information stored on the device. Some cases also involved attackers gaining unauthorised access to compromised systems to carry out further malicious activities. These incidents highlight the continued risk posed by malicious software targeting both individuals and organisations.



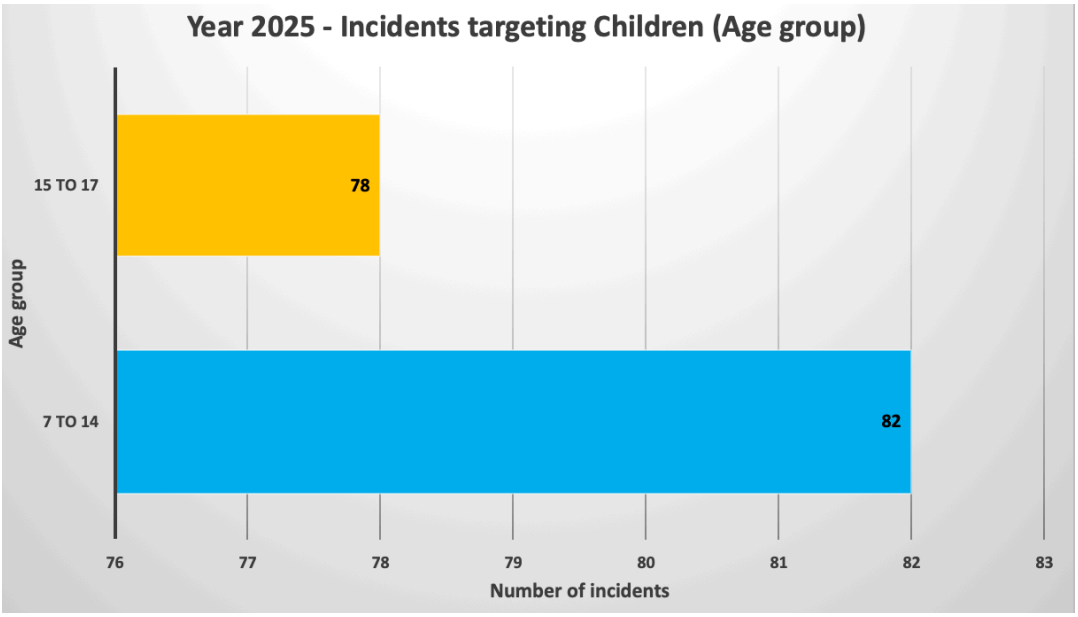
Denial of Service attacks

Only 1% of the incidents were related to Denial-of-Service (DoS) attacks in 2025. These incidents involved attempts to overwhelm online services or websites with a high volume of traffic, resulting in temporary service disruption or reduced system availability. While only a small number of cases were reported through MAUCORS+, such attacks are often underreported, particularly when they affect organisations that manage the incidents internally without public disclosure. As a result, the actual occurrence of DoS attacks may be higher than the figures reflected in the reporting platform.



e) Incidents Targeting Children

The analysis of incidents targeting children reported on the MAUCORS+ platform in 2025 shows that both younger and older minors are exposed to online risks, with a slightly higher number of cases affecting children aged 7 to 14 years. According to the data, 82 incidents were reported for the 7–14 age group, compared to 78 incidents for the 15–17 age group.



The slightly higher number of incidents involving children aged 7 to 14 years are attributed to the increasing use of digital devices, online games, social media platforms, and messaging applications at an earlier age. Children in this age group have limited awareness of online risks, making them more vulnerable to cyberbullying, online harassment, exposure to inappropriate content, and other forms of harmful online interactions.

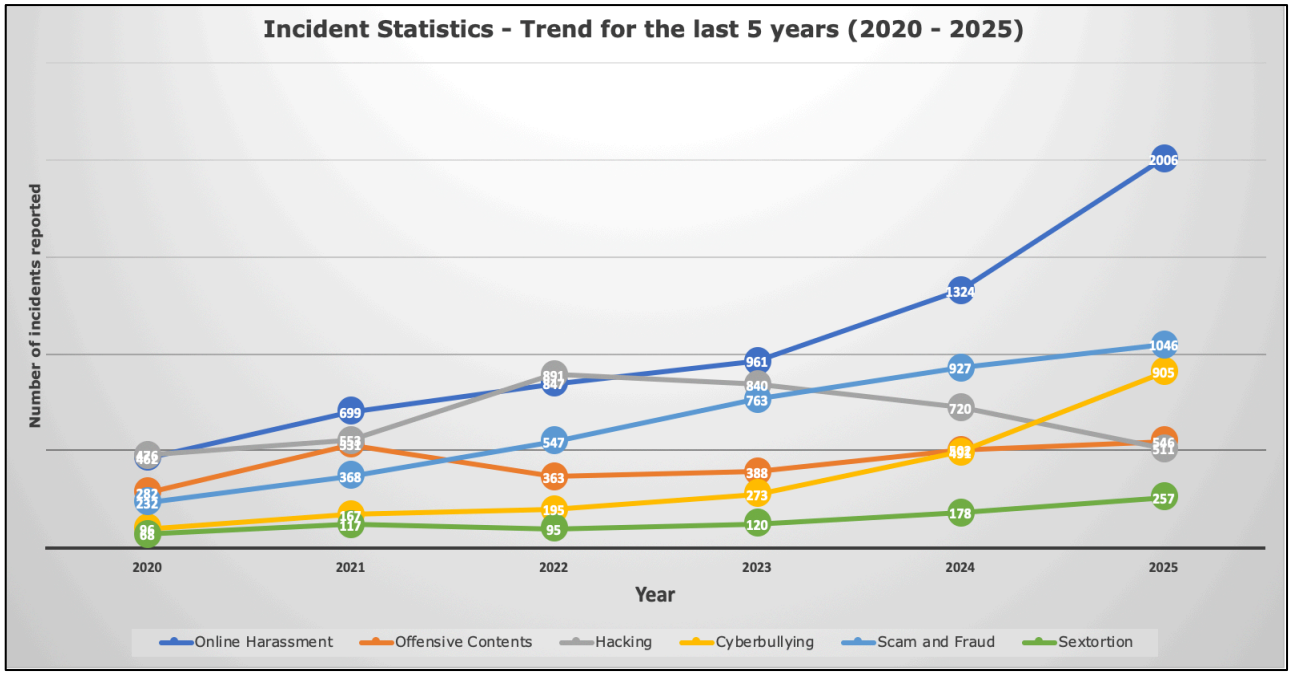
Meanwhile, the 15–17 age group also represents a significant proportion of reported cases. Teenagers in this age bracket are generally more active on social media platforms and online communities, which may increase their exposure to risks such as cyberbullying, online harassment, sextortion, and the misuse of personal images or information.

Overall, the data highlights that online threats affecting children are present across different age groups, underlining the importance of strengthening child online protection measures, digital literacy education, and parental awareness to ensure safer online experiences for young internet users.

8. Comparative Analysis of Incidents

a) 5 Year Trend Analysis of Cyber Incidents (2020-2025)

The data from 2020 to 2025 indicates a clear upward trend in several cyber incidents, particularly those linked to online behaviour and social engineering activities. Most categories show a gradual increase over the six-year period, reflecting the growing use of digital platforms and the increasing exposure of users to online risks.



Online harassment demonstrates the most significant growth during the period. Incidents increased steadily from **462** in 2020 to **2,006** in 2025, showing a sharp and continuous rise. This trend suggests that harassment through digital platforms has become a major concern over the years.

A similar upward trend is observed in cyberbullying, which rose from **96** incidents in 2020 to **905** incidents in 2025. The figures show a consistent increase each year, with a particularly notable rise after 2023. This indicates that harmful online interactions are becoming more prevalent, especially with the widespread use of social media platforms.

Scam and fraud incidents also show a steady and continuous increase over the years. Reported incidents grew from **232** in 2020 to **1,046** in 2025, highlighting the increasing use of digital platforms by cybercriminals to conduct financial scams and fraudulent schemes targeting individuals.

For offensive content, the trend is generally upward, although the growth is less pronounced compared to other categories. Incidents increased from **282** incidents in 2020 to **546** incidents in 2025, with some fluctuations observed between 2021 and 2023.

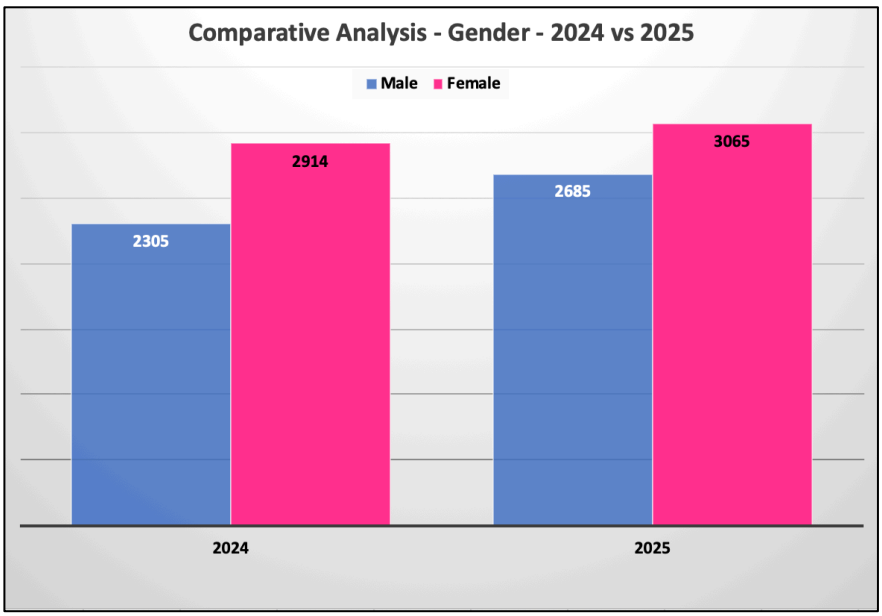
In contrast, hacking incidents show a different trend. Cases increased from **476** incidents in 2020 to a peak of **891** incidents in 2022, after which the numbers gradually declined to **511** incidents in 2025. This may indicate a shift in cybercriminal activities from direct system compromise towards social engineering–based attacks such as scams and fraud.

Finally, sextortion incidents display a gradual upward trend, rising from **68** incidents in 2020 to **257** incidents in 2025, despite a slight decline observed in 2022. The increase in recent years suggests a growing concern related to online exploitation.

Overall, the trend analysis indicates that cyber incidents affecting individuals are increasingly driven by online behaviour, fraud, and social engineering, rather than purely technical cyberattacks.

9. Comparative Analysis for the years 2024 and 2025 – Gender

The comparative analysis of incidents reported on the MAUCORS+ platform in 2024 and 2025 shows an increase in the number of incidents reported by both male and female users. In 2024, 2,305 incidents were reported by men, while 2,914 incidents were reported by women. In 2025, the number of incidents increased to 2,685 for men and 3,065 for women.



The data indicates that female users consistently reported a higher number of incidents than male users in both years. This trend may reflect the higher exposure of women to certain types of online threats, particularly those related to online harassment, cyberbullying, and scams, which are frequently reported on digital platforms.

Between 2024 and 2025, the number of incidents reported by male users increased by approximately 380 cases, while incidents reported by female users increased by around 151 cases. This suggests that while women continue to report more incidents overall, the rate of increase in reported incidents was higher among male users during this period.

Overall, the data highlights that cyber incidents continue to affect both genders, with a consistent trend of higher reporting among women. These findings underline the importance of strengthening online safety awareness, reporting mechanisms, and protective measures to address cyber threats affecting different user groups.

10. Cybersecurity Outlook for 2026 - Mauritius

Based on recent incident trends reported through MAUCORS+, the increasing digitalisation of services in Mauritius, and evolving global cyber threats, the local cyber threat landscape in 2026 is expected to continue shifting toward financially motivated cybercrime and social engineering attacks. As more citizens and organisations rely on digital platforms, cybercriminals are likely to exploit these environments to conduct scams, identity fraud, and other cyber-enabled crimes. The growing sophistication of cybercriminal groups and the use of emerging technologies such as artificial intelligence is also expected to influence the nature of cyber incidents affecting the country.

a) Continued Growth of Online Scams and Fraud

Online scams are expected to remain one of the most dominant cyber threats in Mauritius in 2026. Cybercriminals are increasingly exploiting social media platforms, messaging applications, and online marketplaces to deceive victims through fraudulent schemes, impersonation, and fake investment opportunities. As digital payments and online banking services expand, financially motivated cybercrime is likely to continue targeting individuals and businesses.

b) Rise of Messaging App - Based Scams

Another growing trend expected to continue in 2026 is the use of messaging applications such as WhatsApp and other instant messaging platforms to conduct scams. Cybercriminals increasingly exploit these platforms by impersonating friends, family members, or trusted contacts to request money or sensitive information. In many cases, attackers first compromise a victim's messaging account and then use the contact list to send fraudulent messages requesting one-time passwords (OTP) or urgent financial assistance. The widespread use of messaging applications in Mauritius makes them attractive channels for cybercriminals to quickly reach a large number of potential victims. As a result, scams conducted through messaging platforms are expected to remain a significant cyber threat affecting the public.

c) Increase in Social Media - Based Threats

Incidents involving online harassment, cyberbullying, sextortion, and fake profiles are expected to continue increasing in 2026. The widespread use of social media platforms such as Facebook, TikTok, and Instagram creates opportunities for malicious actors to manipulate users, spread misinformation, or exploit personal information. Young users are likely to remain particularly vulnerable to these threats.

d) Rise of AI-Enabled Scams and Impersonation

With the rapid adoption of artificial intelligence tools globally, cybercriminals are increasingly using AI-generated messages, deepfake audio, and automated phishing campaigns to conduct fraud and impersonation attacks. These technologies allow attackers to produce more convincing scams and operate at a larger scale. As a result, Mauritius may also experience more sophisticated forms of social engineering attacks in the coming years.

e) Increased Targeting of Financial Institutions and Businesses

As Mauritius continues to strengthen its position as an international financial centre and digital economy, financial institutions and businesses may become more attractive targets for cybercriminal groups. Threats such as ransomware, financial fraud, and data breaches are expected to remain a concern, particularly for organisations handling sensitive financial or personal data. Cybercrime is increasingly recognised as a threat to business continuity and financial stability.

f) Growing Risks to Critical Information Infrastructure

The continued digitalisation of government services, telecommunications, healthcare, and other critical sectors may increase the exposure of critical information infrastructures to cyber threats. Cybercriminals and potentially state-sponsored actors may target these sectors to disrupt services or gain access to sensitive information. As cyberspace expands, it continues to be used to conduct fraud, compromise systems, and steal data across borders.

11. 2026 Cyber Threat Trends – Global Level

The global cyber threat landscape in 2026 is expected to become more sophisticated, automated, and driven by artificial intelligence (AI). Cybercriminal groups are increasingly leveraging automation, generative AI, and "cybercrime-as-a-service" models to scale attacks and target both organisations and individuals. As digital transformation accelerates worldwide, threat actors are shifting their focus toward identity-based attacks, social engineering, and financially motivated cybercrime, while continuing to target critical infrastructure and financial systems.

a) Rise of AI-Powered Cyber Attacks

One of the most significant trends expected in 2026 is the increased use of AI by cybercriminals to automate and enhance attacks. AI tools are enabling attackers to generate convincing phishing messages, impersonate individuals using voice cloning or deepfakes, and conduct highly targeted fraud campaigns at scale. AI-supported campaigns already account for a large share of social engineering attacks globally.

Recent reports indicate that deepfake-based impersonation scams and AI-generated fraud attempts are rising sharply, making it increasingly difficult for users to distinguish between legitimate and malicious communications.

b) Continued Evolution of Ransomware

Ransomware is expected to remain one of the most dominant cyber threats globally in 2026, particularly targeting critical infrastructure, healthcare systems, and financial institutions. Threat actors are adopting Ransomware-as-a-Service (RaaS) models that allow less technically skilled criminals to launch attacks using ready-made ransomware tools. Experts also anticipate the growth of data-extortion attacks, where criminals steal sensitive information and threaten to leak it rather than encrypt systems.

c) Expansion of Phishing-as-a-Service and Social Engineering

Phishing continues to be a primary entry point for cyberattacks, accounting for a large share of successful breaches worldwide. By the end of 2025, phishing was responsible for approximately 36–40% of successful cyber intrusions, and this trend is expected to persist in 2026. The emergence of Phishing-as-a-Service (PhaaS) platforms allows cybercriminals to easily launch sophisticated phishing campaigns using pre-built tools capable of bypassing multi-factor authentication and stealing credentials.

d) Growth of Identity-Based and Fraud-Driven Cybercrime

Cybercrime is increasingly shifting toward identity-focused attacks, including account takeovers, synthetic identity fraud, and impersonation scams. Generative AI and large datasets of stolen personal information enable attackers to create highly convincing fraudulent identities and manipulate victims more effectively. Globally, cyber-enabled fraud losses are projected to increase significantly over the coming years as digital payments and online services expand.

e) Increased Targeting of Critical Infrastructure and Supply Chains

Critical infrastructure sectors such as energy, healthcare, telecommunications, and financial services are expected to remain prime targets for cyberattacks in 2026. Supply chain attacks - where attackers compromise third-party software or service providers to gain access to

multiple victims are also likely to increase as organisations become more interconnected digitally.

f) Faster and More Automated Cyber Attacks

Cyberattacks are also becoming faster and more automated, reducing the time defenders have to detect and respond to intrusions. Threat groups increasingly rely on automation and AI-assisted tools to scan vulnerabilities, exploit systems, and move laterally within networks.

12. Staying Ahead with the Evolving Cyber Threats

As the digital landscape continues to expand, cyber threats are becoming more sophisticated, organised, and difficult to detect. Cybercriminals are increasingly leveraging advanced technologies, automation, and social engineering techniques to target individuals, businesses, and critical infrastructures. In this rapidly changing environment, it is essential for both citizens and organisations to remain vigilant and proactive in addressing cybersecurity risks.

Staying ahead of evolving cyber threats requires a coordinated approach that combines awareness, technological measures, and stakeholder collaboration. Continuous cybersecurity awareness and education are crucial in helping users recognise emerging threats such as phishing scams, identity theft, and online fraud. At the organisational level, strengthening cybersecurity governance, implementing robust security controls, and maintaining effective monitoring mechanisms are key to preventing and responding to cyber incidents.

Furthermore, information sharing and collaboration among stakeholders - including government authorities, law enforcement agencies, financial institutions, internet service providers, and the private sector, play a vital role in strengthening national cyber resilience. Timely reporting of cyber incidents and sharing threat intelligence help improve the collective ability to detect, respond to, and mitigate cyber threats.

As digital transformation continues to accelerate, cybersecurity must remain a shared responsibility among all users of digital technologies. By adopting safe online practices, investing in cybersecurity capabilities, and fostering a culture of cyber awareness, both citizens and organisations can contribute to building a more secure and resilient digital ecosystem.

Cybersecurity Good Practices for Citizens

Be Cautious of Suspicious Messages and Requests

Users should remain cautious when receiving unsolicited emails, messages, or calls that request personal information, login credentials, or financial transfers. Cybercriminals often impersonate trusted organisations such as banks, government institutions, or delivery services to deceive victims. Any unexpected request for sensitive information should be treated with suspicion.

Protect Your Online Accounts

Using strong and unique passwords for online accounts is essential. Passwords should not be reused across multiple services. Enabling multi-factor authentication (MFA) wherever available adds an additional layer of security and helps prevent unauthorised access even if login credentials are compromised.

Be Vigilant on Social Media and Messaging Platforms

Given the growing number of scams conducted through messaging applications and social media platforms, users should avoid sharing one-time passwords (OTPs), verification codes, or personal information with anyone. Attackers often compromise accounts and use them to send fraudulent messages to contacts requesting money or sensitive information.

Avoid Clicking on Unknown Links or Attachments

Users should exercise caution when clicking on links or downloading attachments, particularly from unknown or unverified sources. Malicious links may redirect users to fraudulent websites designed to steal personal or financial information.

Keep Devices and Software Updated

Regularly updating devices, applications, and security software helps protect systems from malware and other cyber threats. Software updates often include security patches that address vulnerabilities which could otherwise be exploited by attackers.

Report Suspicious Activities

Individuals who encounter suspicious online activities or fall victim to cyber incidents are encouraged to report the incident through MAUCORS+ (https:maucors.govmu.org) or to the Cybercrime Unit of the Mauritius Police Force. Timely reporting helps authorities respond more effectively and contributes to a better understanding of emerging cyber threats.

Cybersecurity Good Practices for Organisations

Strengthen Cybersecurity Governance

Organisations should establish clear cybersecurity governance structures, including defined roles and responsibilities for managing cyber risks. This includes developing cybersecurity policies, procedures, and risk management frameworks to guide the protection of organisational systems and data.

Implement Strong Access Controls

Access to organisational systems and sensitive data should be restricted based on the principle of least privilege, ensuring that employees only have access to the information necessary for their roles. The implementation of multi-factor authentication (MFA) is also recommended to reduce the risk of unauthorised access.

Regularly Update and Patch Systems

Organisations should ensure that all systems, applications, and network devices are regularly updated with the latest security patches. Many cyberattacks exploit known vulnerabilities that remain unpatched, making timely updates an essential cybersecurity practice.

Conduct Employee Cybersecurity Awareness Training

Human error remains one of the leading causes of cyber incidents. Organisations should therefore provide regular cybersecurity awareness training to employees to help them recognise phishing emails, social engineering attempts, and other cyber threats.

Strengthen Monitoring and Incident Detection

Continuous monitoring of network activity and system logs can help organisations detect suspicious behaviour or potential intrusions at an early stage. Security monitoring tools and incident detection mechanisms should be implemented to enable a timely response to cyber incidents.

Develop and Test Incident Response Plans

Organisations should establish clear incident response plans to ensure a structured and coordinated response in the event of a cyberattack. Regular testing of these plans through cybersecurity exercises or simulations can help improve preparedness and minimise the impact of incidents.

Strengthen Data Protection and Backup Practices

Organisations should implement strong data protection measures, including regular data backups, encryption of sensitive information, and secure storage practices. Backups should be tested regularly to ensure that systems and data can be restored in the event of ransomware or other cyber incidents.

Report Cyber Incidents

Organisations are encouraged to report cyber incidents on MAUCORS+ (https:maucors.govmu.org) or to the Cybercrime Unit of the Mauritius Police Force. Reporting incidents helps authorities monitor emerging cyber threats and provide appropriate assistance where necessary.

13. Conclusion

In the face of a rapidly evolving threat landscape, defending against cyber threats demands constant vigilance and adaptation. Organisations and individuals must stay up to date with emerging threats and refine their defense strategies accordingly. The collaboration of technology, education, and proactive planning form the foundation of a robust cyber defense.

Countering cyber threats necessitates a multi-pronged approach that encompasses diverse strategies. From thwarting phishing attacks to mitigating the impact of ransomware incidents, the key lies in educating users, implementing advanced security measures, and preparing for effective incident response. In this age of digital interconnectedness, safeguarding against cyber threats is not just a responsibility but a crucial imperative to protect sensitive information, preserve operational integrity, and maintain trust in digital interactions.

Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation
Level 3, Wing A
Shri Atal Bihari Vajpaye Tower
Cybercity Ebene
Email: contact@cert.govmu.org