A Review of the 2025 Microsoft Digital Defence Report

The year 2025 marked a significant moment in the evolution of cybersecurity. The Microsoft Digital Defence Report 2025 is published against a backdrop of accelerating digital transformation, the proliferation of artificial intelligence (AI) and a rapidly shifting geopolitical landscape.

The report's central narrative is one of both challenge and opportunity. As organisations, governments and individuals become ever more reliant on technology, the threats they face are growing in both scale and sophistication. At the same time, the tools and strategies available to defenders are also evolving, offering increased resilience and security.

Microsoft argue the cybersecurity is no longer a technical afterthought but a core pillar of economic stability, national security and individual safety. Cyber threats, once the exclusive concern of IT departments, now reverberate through leadership, supply chains and people's daily lives. The pace of change continues to be relentless and the stakes have never been higher.

The Dual Role of AI

A defining theme of the 2025 report is the dual role of artificial intelligence. AI is now both a powerful tool for defenders and a potent weapon for adversaries. On the one hand, AI enables defenders to analyse vast datasets, detect new threats and respond in moments rather than hours. On the other hand, adversaries are leveraging generative AI to enable social engineering, automate lateral movement and evade security controls. The report documents how AI-powered agents are now capable of adapting their tactics on the fly, challenging defenders to move beyond static detection and embrace behaviour-based, anticipatory defence.

At the same time, AI systems themselves have become high-value targets. Adversaries are increasingly employing methods such as prompt injection and data poisoning to attack both models and systems. These attacks can lead to unauthorised actions, data leaks, theft or reputational damage. The report warns that as organisations embrace the strengths of AI, they must also manage its weaknesses and potential exposure, protecting against threats like malicious tool invocation and training data poisoning.

The Threat Landscape

Many of the daily threats organisations face remain familiar, such as opportunistic attacks exploiting known vulnerabilities, phishing and credential theft. However, the methods and scale of these attacks have evolved, driven by the increasing sophistication of threat actors and the growing interconnectedness of digital systems.

One of the most notable developments in 2025 is the widespread adoption of "ClickFix," a social engineering technique that tricks users into executing malicious code themselves, bypassing traditional phishing protections. In 2025, ClickFix accounted for 47% of initial access methods observed by Microsoft Defender Experts, a dramatic rise from its emergence in late 2024. This shift signals a broader trend where attackers are increasingly blending technical exploits with psychological manipulation, making detection and prevention more challenging than ever.

100 trillion

security signals processed by Microsoft every day

The report also highlights the growing use of device code phishing, a technique that exploits the device code authentication flow to capture access and refresh tokens. Both cybercriminal and nation-state actors are leveraging this method to gain initial access, often combining it with targeted social engineering to circumvent traditional detection systems.

Infostealers

The report documents a surge in the use of infostealers, malware designed to harvest credentials and tokens for sale on the dark web. Rather than breaking in, adversaries are logging in, using stolen credentials to gain persistent access. This trend is particularly concerning because it transforms a single infection into a strategic risk,

Research and Education accounted for 39% of all identity compromise incidents

enabling follow-on activities such as ransomware, data exfiltration and extortion. In the first half of 2025, identity-based attacks rose by 32%, with research and education accounting for 39% of all identity compromise incidents.

The cybercrime economy has become highly specialised and scalable, with access brokers playing a pivotal role. These actors specialise in breaching enterprise environments and selling persistent access to other criminals, including ransomware operators, data extortion groups and cyber mercenaries. In the last year, Intel 471 identified 368 access brokers, whose activities affected 68 industries across 131 countries and over 4,000 victims. The majority of these brokers targeted victims in the United States (31%), the United Kingdom (6%) and Thailand (5%).

Expanding Operations

Geopolitical tensions continue to drive a surge in state-sponsored cyber activity. Nation-state actors have expanded their targeting, with a focus on communications, research and education. These sectors, often operating with limited resources, have become strategic incubators for adversarial activity. The report notes that both cybercriminal and nation-state groups are leveraging AI to make their operations more scalable, advanced and targeted.

The geographical distribution of cyber threats reflects broader geopolitical dynamics. The United States (24.8%), United Kingdom (5.6%), Israel (3.5%) and Germany (3.3%) were the most targeted countries in the first half of 2025. Chinese actors focused on IT, government and NGOs, with 35% of attacks targeting the US. Iranian actors directed 64% of their attacks at Israel, while Russian actors expanded their targeting to smaller businesses in NATO countries, with Ukraine as the primary focus. North Korea, meanwhile, has embedded tens of thousands of remote IT workers globally, remitting hundreds of millions of dollars annually to the regime.

Cloud Under Fire

Cloud environments have now moved to become a primary battleground. The volume and sophistication of attacks targeting Azure cloud environments have escalated sharply. In the second 100 days of 2025, there was a 26% increase in incidents compared to the first 100 days and an 87% rise in campaigns aimed at disrupting customer environments through ransomware or mass deletion. Over 40% of ransomware attacks now involve hybrid components, a significant increase from less than 5% two years ago.

Statistical Highlights

The report is rich with data that both quantifies and brings context to evolving threat landscape. Several statistics stand out, especially when compared to the 2024 report:

MFA is still the single most important control

MFA Effectiveness

Multifactor authentication (MFA) continues to block over 99% of unauthorised access attempts, reaffirming its status as the single most important security measure.

Initial Access Vectors

In 2025, 28% of breaches began with phishing or social engineering, 18% with unpatched web assets and 12% with exposed remote services. However, the reliance on exploiting public-facing applications and phishing has declined, while social engineering and supply chain attacks have risen.

Sector Impact

Government agencies, IT and research & academia remain the most targeted sectors. Research and academia, in particular, saw a 32% rise in identity-based attacks.

Ransomware

The overall ransomware picture remains grim. In 2025, 120 ransomware variants were used against 71 industries. Over half of the victims were based in the US, with the UK and Canada following. Data exfiltration occurred in 82% of ransomware incidents, up from previous years.

Password Spray Attacks

Just 20 Autonomous System Numbers (ASNs) accounted for over 80% of malicious password spray activity. 85% of usernames targeted in spray attacks appeared in known credential leaks, with each compromised username appearing in three separate logs on average.

Research and Academia accounted for **49%** of business email compromises in the first half of 2025

AI-Driven Phishing

AI-automated phishing emails achieved a 54% click-through rate, compared to 12% for standard attempts. That's a 4.5x increase. AI-generated IDs used in fraud grew by 195% globally.

The report's second half shifts focus to the defence landscape, articulating a vision for proactive, resilient and collaborative security.

AI-Powered Defence

AI is now essential for detection, response and remediation. Microsoft employs AI to conduct threat analytics, identify detection gaps and automate remediation. AI agents can suspend suspicious accounts, initiate password resets and enforce policies in real time, often acting faster than human responders.

Detection Engineering (or DE) has emerged as a fast-growing discipline in mature cybersecurity organisations. Given the increase in the volume and sophistication of cyberattacks, there is a pressing need for dedicated detection teams. Microsoft has developed a variety of AI solutions to help DE teams effectively manage detections throughout their lifecycle, from threat analysis and identifying detection gaps to authoring and validating detections.

Securing AI Systems

The adoption of generative AI introduces new security imperatives. 57% of organisations experienced an increase in security incidents linked to AI usage. The report advocates for a comprehensive security framework that prepares organisations for AI adoption, discovers how AI is being used, protects sensitive data and systems and governs AI operations with clear policies and safeguards.

Securing AI systems requires a layered defence strategy. At the surface, Small Language Models (SLMs) provide lightweight, high-speed screening of prompts and responses, flagging suspicious patterns at scale. Deeper in the funnel, suspicious signals flow from the SLMs into advanced Large Language Models (LLMs), combined with context from the agent's internal processes. This approach balances efficiency with depth, ensuring both broad coverage and precise decisions.

Disrupting Cybercrime Ecosystems

The disruption of the Lumma Stealer infrastructure in May 2025 exemplifies the power of public-private collaboration. Over 2,300 malicious domains were seized or blocked, reducing the average lifespan of command-and-control servers from 49 days to 18 days. This operation demonstrates that coordinated legal, technical and operational strategies can significantly disrupt cybercriminal ecosystems and protect critical infrastructure.

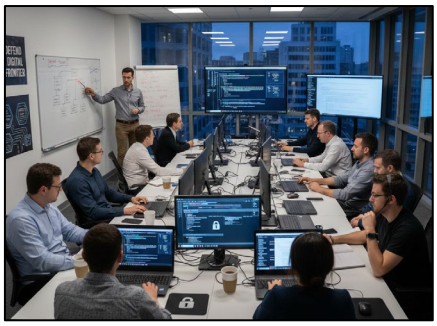
The report also highlights the importance of intelligence sharing. Cyber defence is now a team sport, not an individual one. By sharing and receiving real-time threat data with peers, industry groups and government, organisations can make it harder for cyber adversaries to achieve their goals.

Policy

Governments worldwide are shifting from relying on voluntary guidelines to implementing enforceable standards for cybersecurity. This represents a significant step towards strengthening accountability and ensuring a more robust digital environment. A prime example is the European Union's Cyber Resilience Act, which is set to become a global benchmark for cybersecurity regulation. Much like the General Data Protection Regulation (GDPR) transformed the landscape of data privacy, the Cyber Resilience Act is expected to influence legislation beyond Europe's borders. Its impact will likely prompt organisations around the world to elevate their standards, enhance transparency and adopt best practices for managing cyber risk.

Culture, Training and Collaboration

The report emphasises that technology alone is not enough. Cybersecurity is an organisation-wide effort. Culture and readiness, not just technology, are primary factors in both an organisation's defences and its resilience. The report recommends investing in people, not just tools, and making security part of performance reviews. Upskilling the workforce and embedding security into organisational culture are essential for building resilience.



Collaboration is also key. The report highlights the importance of public-private partnerships, intelligence sharing and cross-sector cooperation. Initiatives like the Global Signal Exchange promote standardised, privacy-conscious frameworks for multi-sector cooperation. Governments are responding to the trillions of dollars lost to scams with legislation

mandating reporting, liability reform and stronger public-private collaboration.

The Impact on Schools

Schools are increasingly targeted by sophisticated cyberattacks, as highlighted in the Microsoft Digital Defence Report 2025. Schools face rising identity-based attacks, where stolen credentials give cyber-criminals access to personal and sensitive data, leading to threats like ransomware and data theft. Cloud services, especially Microsoft Azure, have seen a surge in attacks including mass deletions.

Limited cybersecurity resources make schools vulnerable and technology alone is not enough for protection. The report emphasises that multifactor authentication (MFA) is highly effective, blocking over 99% of unauthorised access, but its use remains inconsistent in education. Schools should prioritise MFA for everyone, alongside regular training to recognise phishing and social engineering, fostering a culture of security awareness and resilience.

Looking Ahead

The Microsoft Digital Defense Report 2025 concludes with a call to action. Security is a shared responsibility, requiring collaboration across borders, sectors and disciplines. The insights and data presented throughout the report underscore the urgency of transparency, innovation and collective action. As threats evolve, so too must our defences, strategies and partnerships.

The report's closing message is clear. As global regulatory frameworks evolve and legislative trends reshape the cybersecurity landscape, one thing remains constant. Security is a shared responsibility.

A security researcher may earn $10,000 for responsibly disclosing a vulnerability to a bug bounty program, but may earn over $100,000 by selling the same exploit to a cyber mercenary.

References

- Microsoft Digital Defence Report 2025 (Link)
- DfE Digital and Technology Standards for Schools (Link)
- National Cyber Security Centre guidance for schools (Link)

About Virtue Technologies

Virtue Technologies is an education-focused IT company with nearly two decades of experience partnering with schools to deliver tailored technology solutions. Established in 2006, the company has become a leading provider of IT services for Primary and Secondary Schools and Multi Academy Trusts. Their key areas of expertise are Support, Cyber Security, Cloud Solutions and Classroom Productivity.

With a clear commitment to enhancing educational outcomes through technology, Virtue Technologies collaborates closely with academic institutions to understand their unique needs and challenges. The company emphasises building long-term partnerships, ensuring that each solution not only aligns with current requirements but also anticipates future growth. Their dedicated team of professionals stays abreast of technological advancements, allowing them to introduce innovative practices and resources into classrooms efficiently. Over the years, Virtue Technologies has earned a strong reputation within the educational sector for reliability, adaptability and exemplary customer service. By focusing on continuous support and professional development, they empower educators and administrators to make the most of their IT investments, fostering enriching learning environments for students across all levels of education.

About the Author

Will Stead has over 35 years of experience in IT management and leadership, spending the last 15 years specialising in the education sector, supporting schools and Multi Academy Trusts across the UK.

Will's expertise lies in developing and implementing IT strategies tailored for both individual schools and MATs. He works directly with school leadership teams and IT departments to create strategic plans that drive digital transformation, improve classroom productivity and ensure robust cybersecurity practices. His approach is highly collaborative, focusing on building strong relationships and trust with stakeholders to deliver technology solutions that are both effective and sustainable.

Contacting Virtue Technologies

www.virtuetechnologies.co.uk

01695 731233

info@virtuetechnologies.co.uk