TIEVA

FULCRUM IT PARTNERS

CYBER NEWS

Stay Secure: The Latest in Cyber News & Updates

THREATS

NEWS

MORE

August 2025 - VOL.5

TIEVA
FULCRUM IT PARTNERS

Cyber News

INTRODUCTION

Welcome

Packed with the latest cybersecurity news, insights into emerging threats, free tools you can leverage, and expert analysis you can trust—Cyber News is designed to keep you informed and protected in an ever-evolving digital landscape.

Written by seasoned professionals, each edition brings you practical guidance, industry updates, and actionable tips to help you stay one step ahead. Whether you're an IT leader, security analyst, or simply passionate about digital safety, there's something here for you.

Let’s dive in - This Is TIEVA Cyber

TIEVA
FULCRUM IT PARTNERS

Cyber News

NEWS & EMERGING THREATS

News

The fall of XSS[.]is

In a major win for international cybercrime enforcement, Ukrainian security services supported by French police and Europol arrested the suspected administrator of the Russian-language forum XSS[.]is in Kyiv on 22 July 2025. The four-year investigation, which began in France in July 2021, used intercepted Jabber communications via thesecure.biz. The suspect allegedly earned over €7 million through mediating illicit transactions, resolving disputes, and running encrypted platforms. XSS[.]is, active since 2013 with over 50,000 users, had enabled the sale of malware, stolen data, and ransomware services. Its takedown strikes a major blow to the global cybercrime landscape. XSS[.]is arrested

Microsoft Teams weaponised

Cybercriminals recently exploited Microsoft Teams to deliver Matanbuchus 3.0 malware in a targeted ransomware campaign. Disguised as IT support during Teams calls, attackers tricked users into running a remote support script that silently installed the malware. Once deployed, Matanbuchus gathered system data and maintained persistence via scheduled tasks, all while evading detection. The incident highlights how trusted platforms like Teams can be weaponised. As remote collaboration grows, organisations must remain alert to increasingly deceptive threats that exploit employee trust and internal tools. Teams call weaponised

SharePoint – Cyber espionage in action

Microsoft has linked a series of recent attacks on on-premises SharePoint servers to Chinese state-affiliated threat groups. The attackers exploited two zero-day flaws CVE-2025-53770 and CVE-2025-53771 enabling remote code execution and persistent access. Active since early July, the campaign has affected multiple sectors, including US government agencies. The exploits are attributed to Linen Typhoon, Violet Typhoon, and Storm-2603, all known for cyber-espionage. Microsoft is urging immediate patching and credential rotation, warning that unpatched systems remain highly vulnerable.

Sharepoint on-premies vulnerabilities

Emerging Threats

Mobile malware is rising sharply, with over 12 million attacks blocked in the first half of 2025 alone. The most common threats include trojans, spyware, adware, and ransomware, often disguised as legitimate apps or delivered via phishing messages. Rising threat of moblie malware

Agentic AI driven attacks are accelerating in 2025, with autonomous cyber agents carrying out tasks like phishing, credential stuffing, and reconnaissance with little to no human input. These attacks are highly scalable and adaptive, allowing threat actors to launch broader campaigns faster and with greater precision. Agentic AI attacks

Credential theft has reached staggering levels, with billions of items stolen during 2024, a significant increase year-over-year. This trend has accelerated in 2025, with threat actors employing multiple infostealers installed by single loaders, maximizing their harvest from each successful breach.

Identity theft surge

Cyber News

NEW VULNERABILITIES

CVEs

CVE Vulnerabilities Update. In this section, we highlight the latest discovered vulnerabilities (CVE) affecting a wide of systems and applications. Stay informed about these critical security threats to ensure you're equipped to protect your environment from emerging risks.

CVE-2025-49704 - Microsoft SharePoint Exploitation Chain

Description: This vulnerability arises from improper control of code generation (CWE-94), allowing an authenticated attacker with low privileges to execute arbitrary code remotely on vulnerable on-premises SharePoint servers. NIST Link

9.8 Critical

CVE-2025-41238 – VMware PVSCSI Heap Overflow Vulnerability

Description: VMware ESXi, Workstation, and Fusion contain a heap-overflow vulnerability in the PVSCSI (Paravirtualized SCSI) controller that leads to an out of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. Vendor Advisory ID: VMSA-2025-0013. NIST Link

9.3 Critical

CVE-2025-5777 – Citrix NetScaler Memory Disclosure Vulnerability

Description: This vulnerability, dubbed CitrixBleed 2, affects Citrix NetScaler ADC and Gateway appliances. It stems from insufficient input validation, allowing unauthenticated attackers to send specially crafted HTTP requests that trigger out-of-bounds memory reads. NIST Link

9.3 Critical

CVE-2025-20337 – Cisco ISE & ISE-PIC SQL Injection

Description: This vulnerability is a critical remote code execution vulnerability in Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC). It allows unauthenticated attackers to execute arbitrary commands as root on affected systems by exploiting a flaw in a specific API endpoint. NIST Link

9.3 Critical

For assistance remediating these or any vulnerabilities please call 0333 043 0333

TIEVA
FULCRUM IT PARTNERS

Cyber News

Case Study

Tech Support Scam Surge in the UK

The UK is currently facing a surge in tech support scams, driven by the widespread reuse of stolen credentials from historic data breaches. Since early 2025, cybercriminals have been actively exploiting massive credential dumps circulating on dark web forums and Telegram groups. These data sets, some dating back over a decade, include email addresses, partial passwords, and other sensitive user identifiers. Financial institutions and telecom providers are reporting escalating scam attempts, prompting **the National Cyber Security Centre (NCSC)** to issue an urgent advisory in July warning of the growing threat. chain.

Attackers are using leaked data to convincingly impersonate trusted brands like Microsoft, Apple, BT, and major banks. Victims are being targeted through cold calls, phishing emails, and pop-up messages designed to mimic legitimate security alerts . Once engaged, the scammers instruct users to call **fake support lines** or download remote access tools. From there, they persuade victims to reveal passwords, credit card information, National Insurance numbers, or one-time passcodes, effectively bypassing standard authentication protections.

This campaign is actively affecting thousands of UK businesses. According to ongoing reports, over **400,000 individuals** have been targeted in the first half of the year, with **more than £5.8 million in confirmed fraud losses.**

Vulnerable groups such as older adults are disproportionately impacted. Although these scams are not caused by new breaches, they repurpose old, forgotten data to carry out new and highly effective fraud attempts, putting both personal identities and financial assets at risk.

UK-based telecoms including **BT and Sky** are actively intervening by alerting customers and blocking known spoofed phone numbers associated with offshore scam centers. The **NCSC** continues to advise users to verify unsolicited IT support contact and avoid granting remote access without due process. Financial regulators and banks are also pushing emergency changes to authentication processes, including callback verifications and non-SMS-based multi-factor authentication.

This ongoing threat underscores the importance of long- term data security and public vigilance. Attackers continue to exploit trust, outdated data, and technical gaps to manipulate users, making **cyber awareness and shared accountability** essential. The UK cybersecurity community, financial sector, and telecom providers must remain coordinated and proactive in their response. Without persistent monitoring, education, and enforcement, these scams are likely to evolve further and remain a sustained threat well into the coming months.

↓ REMEMBER

TIEVA support will never call you out of the blue. Always ask for the ticket number from an email.
TIEVA support will never ask for payment. This is always a red flag.
TIEVA support will never ask for your password or personal identifiers.
Not sure? Call us directly at 0333-043-0333 or email servicedesk@tieva.co.uk

TIEVA
FULCRUM IT PARTNERS

Cyber News

Service

Cybersecurity Assessment. Be proactive, not reactive

The threats and impacts of evolving cyber-attacks and risks continues to evolve. Regardless of source, organisations require constant vigilance, not only in preventing breaches, but also identifying and responding to incidents as early as possible to protect their environment.

From ransomware to regulatory pressure, organisations face escalating threats that demand more than basic security hygiene. Business and IT leaders are expected to protect sensitive data, maintain service continuity, and demonstrate cyber maturity, all while managing tight budgets, limited time, and stretched internal resources.

Security Assessments are designed to help organisations evaluate their risk profile and cybersecurity maturity. Understanding the strengths and gaps in your security programme offers multiple benefits, including identifying challenges, uncovering opportunities, and improving service levels.

Investing in a Cyber Security Assessment isn't just smart it's crucial to provide confidence and a clear, actionable understanding of your current readiness and resilience against cyber incidents.

Reach out to talk about Assessments:
0333 043 0333

KEY ADDITIONAL BENEFITS:

Emerging Threats: Stay ahead of emerging threats by annually assessing your systems against a recognised security framework.

Identify Gaps: Security Assessment can help Identify gaps in documentation, security policies, and controls.

Security Roadmap: Provide your organisation with an actionable roadmap with clear objectives to help achieve the desired security posture.

TIEVA

FULCRUM IT PARTNERS

Cyber News

Quick Wins

MXTOOLBOX®

Secure Your Email with MXToolbox

Without proper email authentication, criminals can spoof your domain, your emails may be marked as spam, and your reputation suffers. SPF (Sender Policy Framework) defines which servers can send on your behalf. DKIM (DomainKeys Identified Mail) verifies your emails haven't been altered and come from an authorised source, and instructs receiving servers how to handle failed checks.

How to Check Your Email Security

Step 1: Test Your SPF Record

- Go to mxtoolbox.com/spf.aspx
- Enter your domain (e.g., yourcompany.com)
- Click "SPF Record Lookup“

Step 2: Check DKIM Setup

- Go to mxtoolbox.com/dkim.aspx
- Enter your domain
- Try selectors: "default", "selector1", or "google"
- Click "DKIM Lookup“

Step 3: Verify DMARC Policy

- Go to mxtoolbox.com/dmarc.aspx
- Enter your domain
- Click "DMARC Lookup"
- Understanding Your Results
- All Green ✅: Excellent! Your email authentication is properly configured.
- Mixed Results ⚠️: You have some protection, but gaps remain. Address red flags first.
- All Red ❌: Your domain is vulnerable to spoofing. Urgent action required.

Quick Fixes

Missing SPF? Contact your IT team or email provider. Start with monitoring mode:

- Microsoft 365: v=spf1 include:spf.protection.outlook.com ~all
- Google Workspace: v=spf1 include:_spf.google.com ~all

Important: The ~all (soft fail) allows monitoring without blocking emails. Never use -all without first identifying ALL systems that send email from your domain.

No DKIM? Enable through your email provider's admin console—most offer one-click setup.

Missing DMARC? Start with monitoring: v=DMARC1; p=none; rua=mailto:your-email@yourcompany.com

The Business Impact

Proper email authentication delivers:

- Improved delivery to inboxes, not spam folders
- Brand protection against impersonation
- Customer trust in your communications
- Compliance with industry requirements

Take Action Today:

Run these three MXToolbox tests now.

Need help implementing these fixes? Contact us for a free email security assessment.

TIEVA

FULCRUM IT PARTNERS

Cyber News

THOUGHT OF THE MONTH

The Online Safety Bill: Striking the Balance Between Safety, Security, and Anonymity

The UK's newly enacted Online Safety Bill marks a major shift in digital regulation—aiming to reduce online harm, protect children, and hold platforms accountable. However, its sweeping scope raises concerns around surveillance, privacy, and the future of online anonymity.

One immediate effect is the rapid rise in anonymised VPN usage, as users seek to bypass increased monitoring and content filtering. While these tools provide privacy, they also create cybersecurity challenges for businesses and public sector organisations. Risks include hidden data exfiltration, reduced network visibility, and the ability to sidestep firewalls and compliance safeguards. In response, companies must strengthen VPN policies, employee training, and monitoring practices—but without assuming all anonymity

Indeed, the right to remain anonymous online is vital for whistleblowers, journalists, abuse survivors, LGBTQ+ individuals, and others who rely on privacy for safety and free expression.
The Bill's pressure on platforms to pre-emptively moderate content could incentivise intrusive tracking—potentially undermining legitimate anonymity and creating a chilling effect

What can be done?

- Apply nuanced VPN policies (restrict risky consumer tools while supporting secure enterprise-grade VPNs)
- Deliver user education on VPN risks, privacy, and policy obligations
- Retain anonymous access routes for vulnerable users within safe, accountable frameworks

Final Thoughts

The path forward lies in balance. Organisations should apply nuanced VPN policies, invest in privacy-respecting monitoring, educate users, and defend anonymity where genuinely required. As the Online Safety Bill begins to reshape the UK's digital landscape, cybersecurity must evolve in a way that safeguards both safety and fundamental digital rights..

If you're unsure how the Online Safety Bill will impact your network policies or privacy posture, we're here to help.

Contact us

If you'd like to discuss how to strengthen your cybersecurity posture, our experts at TIEVA are here to help.

Contact us today to explore tailored solutions that protect your business from modern cyber threats.

Email TIEVA
hello@tieva.co.uk

Call TIEVA
+44(0) 333 043 0333

Find out more
www.tieva.co.uk

TIEVA
FULCRUM IT PARTNERS