TIEVA

FULCRUM IT PARTNERS

CYBER NEWS

Stay Secure: The Latest in Cyber News & Updates

THREATS

NEWS

MORE

November 2025 - VOL.7

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

Ransomware Attack Disrupts Operations at Major European Airports

A ransomware attack on Collins Aerospace's MUSE check-in system caused major disruption at several European airports, including Heathrow and Brussels, between 22 - 25 September. The incident affected key passenger processing systems, resulting in flight delays and operational impact across multiple airlines.

Initial investigations suggest backend systems were encrypted, with data such as passenger details and baggage records potentially exfiltrated. A suspect has been arrested in the UK in connection with the attack. Collins Aerospace is working with airline partners and cybersecurity authorities to restore services and strengthen system resilience.

Ransomware-on-Collins-Aerospace

Miljödata Breach by DataCarry Exposes Volvo Employee and HR Data

The DataCarry ransomware group has claimed responsibility for a breach of Swedish HR software provider Miljödata, resulting in the exposure of personal data belonging to over 1.5 million individuals. Among the affected are Volvo employees, whose compromised information reportedly includes names, national ID numbers (SSNs), addresses, and employment details.

The breach is believed to have occurred through exploitation of an unpatched vulnerability in Miljödata's infrastructure. Stolen data is now being advertised on ransomware leak sites. Authorities in Sweden have launched an investigation, and impacted organisations are being urged to notify affected individuals and review third-party data handling practices.

Miljödata | Search the Data Breach

Critical Vulnerabilities in Cisco Firewalls and VPNs Actively Exploited

Two critical security flaws (CVE-2025-20333 and CVE-2025-20362) affecting Cisco firewalls and VPN devices are being actively exploited by threat actors. These vulnerabilities allow unauthorised remote access and remote code execution, potentially giving attackers full control over affected systems.

Cisco has released security updates to address the issues and strongly urges all users to apply patches immediately. Organisations relying on these devices should also monitor network activity for signs of compromise and review their security configurations.

Cisco Critical Vulnerabilities - VPNs - Firewalls

Emerging Threats

APIs: An Overlooked Target in Modern Cyber Attacks

APIs have become an essential part of how systems communicate connecting everything from mobile apps and payment systems to CRMs and cloud platforms. But as their use has expanded, so has the interest of attackers.

Instead of exploiting traditional network or application vulnerabilities, threat actors are increasingly targeting APIs to abuse functionality, access sensitive data, or bypass controls. These attacks often exploit business logic flaws, which can be difficult to detect with standard security tools.

How SMEs Can Protect Themselves:

- Maintain a complete inventory of all APIs in use.
- Apply strong authentication and access controls to every API endpoint
- Use API gateways and monitoring tools to detect unusual behaviour or traffic spikes
- Limit data exposure by ensuring APIs only return what's necessary
- Review and test APIs regularly, especially for business logic and authorisation issues

TIEVA
FULCRUM IT PARTNERS

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-2025-20333 – Cisco ASA Authentication Bypass

Description: FreePBX versions 15, 16, and 17 contain critical authentication bypass and SQL injection vulnerabilities allowing unauthenticated remote attackers to gain administrative access and execute arbitrary code. This affects the web-based management interface used to configure telephony systems. NIST Link

10.0 Critical

CVE-2025-7775 - Citrix NetScaler Memory Overflow

Description: Memory overflow vulnerability in NetScaler ADC and Gateway appliances that could allow unauthenticated remote code execution and denial of service. Affects appliances configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual. NIST Link

9.2 Critical

CVE-2025-55177 - WhatsApp Device Synchronization

Description: Incomplete authorization of linked device synchronization messages in WhatsApp for iOS and Mac could allow unrelated users to trigger processing of content from arbitrary URLs on target devices. Exploited in combination with Apple vulnerability for sophisticated spyware attacks. NIST Link

8.0 High

CVE-2025-43300 - Apple ImageIO Out-of-Bounds Write

Description: Out-of-bounds write vulnerability in Apple's ImageIO framework affecting iOS, iPadOS, and macOS. Processing malicious image files may result in memory corruption. Used alongside WhatsApp vulnerability in targeted attack campaigns. NIST Link

8.8 High

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

TIEVA

FULCRUM IT PARTNERS

Cyber News

CASE STUDY

Microsoft Direct Send – Exploitation on the rise

Microsoft 365

Recent security research has revealed that Microsoft 365's Direct Send feature is being actively exploited by cybercriminals, posing a significant and growing risk to UK organisations.

Originally intended to simplify email delivery from devices and applications, Direct Send is now being abused by threat actors. Security researchers at Proofpoint, Varonis, and Mimecast have documented campaigns where attackers use Direct Send to send spoofed emails that appear to come from trusted internal sources, bypassing authentication and security controls.

The impact is already being felt across sectors. In recent months, over 70 organisations globally including several in the UK have reported incidents where attackers leveraged Direct Send to distribute convincing phishing emails. In one documented case, attackers used Direct Send to send internal-looking phishing emails that led to credential theft and unauthorised access to sensitive systems. Because these emails are routed through Microsoft's trusted infrastructure, they often evade perimeter security and appear as legitimate internal messages.

Security vendors have observed attackers using business themed lures, such as payment requests and voicemail notifications, to trick users into divulging credentials or authorising fraudulent transactions. Microsoft and leading security experts now recommend disabling Direct Send unless strictly necessary, restricting it to approved IPs, and implementing sender validation.

To reduce risk, organisations should regularly review mail flow configurations, restrict Direct Send to approved IP addresses, and implement sender validation wherever possible.

Just as important is ongoing staff awareness training, so employees know how to spot suspicious request even when they appear to come from trusted sources.

In the current threat landscape, a combination of technical controls and vigilant processes remains the most effective defence.

Check your environment today to ensure restrictions are in place against a Microsoft Direct Send exploit or contact TIEVA for assistance

TIEVA
FULCRUM IT PARTNERS

Cyber News

SERVICE

Optimise Your Infrastructure:
Network Assessment Made Simple

Your network is the foundation of your organisation's digital operations. As demands grow and environments evolve, visibility into your infrastructure becomes essential.

TIEVA's Network Assessment Service helps businesses uncover hidden risks, optimise performance, and plan confidently for the future.

Whether you're preparing for a cloud migration, rolling out new applications, or simply maintaining operational resilience, understanding your network is key. TIEVA's modular service provides tailored insights into wired, wireless, and cloud environments delivered by certified network engineers and architects.

Why Assess Your Network

Networks evolve over time. New devices, changing business priorities, and expanding teams can introduce complexity and hidden inefficiencies. Without a clear picture of your environment, even small issues can snowball into major disruptions.

TIEVA's Network Assessment helps you:

- Understand the impact of business projects on network performance
- Identify opportunities for optimization
- Align infrastructure with business and technical objectives

To talk about a Network Assessment Call:
0333 043 0333

KEY OUTCOMES:

End-to-End Visibility: Comprehensive understanding of network assets, configurations, and performance.

Actionable Recommendations: Clear next steps aligned to business and technical objectives.

Strategic Planning Confidence: Roadmaps and data to support transformation, budgeting, and board-level reporting.

Governance & Risk Insight: Gap analysis across cost, security, identity, and operational controls.

TIEVA
FULCRUM IT PARTNERS

Cyber News

QUICK WINS

PhishTank

PhishTank is a free, community-driven database of verified phishing websites. When you receive a suspicious email with a link, PhishTank lets you check if that link is a known phishing site before you click it.

Step 1: Copy the Suspicious Link (Don't Click It!)

Step 2: Check on PhishTank
Go to https://phishtank.org
Paste the URL in the search box
Click "Is it a phish?"

Step 3: Read the Results
"Not found in PhishTank database"

- Not currently listed as phishing
- Still use caution and check other warning signs
- "This is a known phish"
- Confirmed malicious site
- DO NOT click the link
- Delete the email immediately or follow your organisation's reporting process.

What PhishTank Shows You:

- Whether a URL is a confirmed phishing site
- When it was first reported
- Who verified it
- How many people confirmed it's malicious

Important Caveats
Not finding a URL doesn't mean it's safe – PhishTank contains millions of phishing sites, but new ones appear daily. If a URL isn't listed but still looks suspicious, don't click it.

Shortened URLs need expanding first - Links like bit.ly or tinyurl.com hide the real destination. Use a URL expander service (unshorten.it) to reveal the actual URL before checking.

PhishTank is reactive, not proactive - A site must be reported and verified before it appears in the database. Brand new phishing sites won't be listed yet.

Still use your judgment - Also watch for:

- Generic greetings ("Dear customer")
- Spelling errors in the email
- Urgent or threatening language
- Sender address doesn't match claimed company

Verify independently: Even if PhishTank confirms a link is safe, if the email requests sensitive information, verify through another channel,call the sender directly

Report new phishing: If you find a phishing site not in PhishTank, you can submit it (free account required). Your submission helps protect others.

UK reporting: Forward phishing emails to report@phishing.gov.uk (NCSC's Suspicious Email Reporting Service).

Over 80% of cyberattacks begin with phishing emails. PhishTank gives you a simple, 30-second way to verify suspicious links before clicking.

Need to secure your email? Contact us for further information and assistance.

TIEVA

FULCRUM IT PARTNERS

Cyber News

THOUGHT OF THE MONTH

Collateral Damage: When a Supplier Breach Becomes Your Problem

Major organisations are increasingly finding themselves exposed through their extended networks. Across sectors, attackers are shifting focus from direct intrusions to weaknesses in suppliers, service providers, and software partners.

A single compromised update or misconfigured vendor system can trigger widespread disruption halting production lines, delay deliveries, and exposing sensitive data.

The MOVEit file transfer breach and the Okta support incident showed how quickly a single supplier vulnerability can ripple across hundreds of clients, while attacks on manufacturing firms such as Vauxhall's logistics partner and Jaguar Land Rover's supply chain highlight the real-world impact of third-party compromise.

Smaller firms within supply chains remain soft targets, they hold valuable access but often lack the layered defences of their enterprise clients.

Once inside, threat actors can move laterally, using legitimate third-party credentials to bypass trust boundaries and remain undetected. These indirect attacks are proving both harder to contain and more damaging, underlining how interconnected risk has become across the UK's digital economy.

What can be done?

- Strengthen visibility across your vendor network. Map out every third-party connection, limit privileged access and apply multi-factor authentication as standard. Monitor supplier accounts for unexpected activity or unusual data transfers.
- Train teams to question unexpected supplier requests and verify communication channels before acting. Real-world simulation exercises can help employees recognise and report threats early.
- Test response plans jointly with key partners. Clear escalation routes and shared communication protocols can make all the difference when a supplier incident impacts your operations..

Final Thoughts

No organisation operates in isolation. Each supplier, platform, and partner adds both value and risk. Building resilience means strengthening those connections, demanding transparency, and planning for failure. When every link in the chain understands its role, the whole network becomes harder to break.

Whether it's supply chain risk, ransomware resilience, or shifting compliance needs, TIEVA is ready 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