TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

January 2026

Cyber weather

Cyber weather gives you an update on the key information security incidents and phenomena of the month.

The product is primarily targeted at those who work with information security issues at different levels of organisations. Cyber weather gives readers a quick overview of recent and upcoming events in the field of cyber security.

Cyber weather can be: ☀ calm 🌧 worrying ⛈ serious

Overview of cyber weather in January 2026

January was rainy

The month's cyber weather was once again shaped by vulnerabilities discovered in network edge devices from various manufacturers, with exploitation observed worldwide.

In addition, phishing messages aimed at hijacking Microsoft 365 accounts continued to circulate in large numbers. Detecting M365 account breaches is difficult without active system monitoring and analysis of login logs.

During the reporting period, an exceptional data breach came to light in which the attacker is reported to have had unauthorised access to an energy sector company's web service for nearly a year. The case was uncovered when unauthorised content was detected on the company's website.

- According to public reporting, the attacker may have accessed approximately 31,000 electricity contract records in Finland.

January also saw increased discussion around the growing use of AI assistants in organisations, along with the associated information security and cybersecurity challenges that must be considered when planning their deployment and use. We published an article compiling key considerations and recommendations for the secure and responsible use of AI assistants.

Review of 2025

Compiled by experts at the NCSC-FI, the publication *Kyberturvallisuuden vuosi 2025* (Cybersecurity Year 2025) provides an overview of the key cyber threats that affected Finland during the year. The review also offers guidance for organisations on what 2026 may bring and what measures the evolving threat landscape is likely to require.

NCSC-FI's tips and recommendations for improving cybersecurity preparedness

High expectations are currently being placed on autonomous AI agents. At the same time, more advanced automation powered by large language models introduces new cybersecurity risks. New guidance developed by Traficom and the National Emergency Supply Agency helps organisations design, build and maintain agentic AI systems securely.

Traficom's trend report highlights three key trends in transport, communications and cybersecurity that require attention in the coming years. As society becomes increasingly digitalised, cybersecurity is becoming an ever more important component of comprehensive security.

The EU-funded SECURE project is providing financial support for small and medium-sized enterprises to support the implementation of the Cyber Resilience Act (CRA). European SMEs subject to the obligations of the CRA are eligible to apply. The application period is open until 29 March 2026.

The Ministry of Finance and Traficom are jointly developing an assessment framework, or a national library of assessment criteria, for public administration cloud services (*Kansallinen kriteeristöpankki*, KriPa) to support authorities in managing risks related to cloud services and to promote the appropriate protection of security classified, non-disclosable and public information. The work is scheduled to be completed in autumn 2026.

Icy shower of the month

Large-scale cyberattacks against Poland’s energy infrastructure

On 29 December, multiple targets within Poland’s energy infrastructure were hit by a large-scale, coordinated cyberattack aimed at destroying systems and data. The attackers had likely established a foothold months before carrying out the destructive actions. Poland’s cybersecurity authority published a report on the incident in January. [14]

The attacks primarily targeted connection points between renewable energy production facilities and electricity distribution system operators (DSOs), where network edge devices and industrial automation systems used to control the power grid are located. Distribution operators lost visibility and control over these connection points. Data was destroyed from workstations and servers at heat and power generation facilities, and some devices were rendered inoperable.

Despite the severity of the incident, it did not affect electricity or heat production, nor the overall functioning of Poland’s power system.

Widespread attention

- According to the Polish report, indicators of infrastructure associated with state-sponsored threat actors were identified in the attacks.
- This marks the first large-scale destructive cyberattack targeting the energy infrastructure of an EU Member State. Similar attacks have previously been observed in Ukraine.
- The incident has sparked discussion about the importance of protecting critical infrastructure, managing risks and implementing good security practices — including in Finland.

Cyber weather phenomena

In this section,
we review developments and trends
in key cybersecurity phenomena.

1 mo.

Cyber weather
January 2026

Data breaches and leaks

January was largely calm. Reports of Microsoft 365 account breaches increased towards the end of the month. An energy sector website was compromised, resulting in the exposure of personal data.

Malware

During January, the NCSC-FI received reports of malware distributed in connection with various phishing campaigns. However, the number of reports remained moderate.

Vulnerabilities

Several zero-day vulnerabilities were exploited in data breaches during the month.

Scams and phishing

Convincing scams impersonating the Finnish Patent and Registration Office (PRH) targeted entrepreneurs. The fraudulent messages urged recipients to update their company details.

A new SMS scam warns of a suspicious bank transaction and instructs recipients to call a provided phone number.

Automation and IoT

The cybersecurity authorities of Australia and six other countries have jointly developed guidance on establishing secure network connections for industrial automation. The guidance forms part of a joint publication series focused on securing production environments.

Network performance

The largest botnets used for denial-of-service attacks continue to grow in scale and capability. A major contributing factor is poorly secured consumer devices.

1 mo.

Cyber weather
January 2026 1/2

Data breaches and leaks

- January was calm in terms of data breach reports.
- Reports of Microsoft 365 account breaches increased towards the end of the month.
- An energy sector organisation’s website was compromised, with unauthorised articles published and some personal data exposed.
- The NCSC-FI received reports of WhatsApp and Telegram account takeovers and attempted takeovers. The number of reports declined towards the end of the month.
- Several data breaches were also carried out by exploiting zero-day vulnerabilities in multiple products.

Malware

- January was otherwise quiet in terms of malware detections. However, the NCSC-FI received reports of infostealer malware distributed as attachments in various phishing messages. These were circulated, for example, via messages on the Discord platform.
- Malware traffic linked to different botnets continues to be observed in Finland. Device security improves when devices are kept up to date and purchased from reputable manufacturers. Users should avoid unnecessary remote access connections and install software only from trusted sources.

Vulnerabilities

- A vulnerability in the MongoDB database software allows confidential information to be disclosed. (CVE-2025-14847)
- A critical vulnerability was identified in FortiOS, FortiManager, FortiProxy and FortiAnalyzer products. Exploitation has also been observed in Finland. (CVE-2026-24858)
- Critical vulnerabilities were also identified in Ivanti Endpoint Manager Mobile (EPMM). Exploitation of these vulnerabilities has been observed globally. (CVE-2026-1281 and CVE-2026-1340)

1 mo.

Cyber weather
January 2026 2/2

Scams and phishing

- Convincing scams impersonating the Finnish Patent and Registration Office (PRH) targeted entrepreneurs. The fraudulent messages urged recipients to update their company details, but the link redirected users to a criminal-controlled website instead of the official PRH service.
- Text message scams have adopted a new theme, warning victims of a suspicious bank transaction and instructing them to call a provided phone number. The number does not connect to a bank, but to a criminal fraudster.

Automation and IoT

- Internationally coordinated guidance presents eight recommended cybersecurity principles for designing and establishing network connections in industrial automation. These cover, among other things, risk management, connection policies and governance, and limiting the impact of attacks.
- Insufficient or misconfigured protections of production environment network connections have also led to security incidents in Finland.

Network performance

- No serious disruptions were observed in public communications networks in January.
- In recent years, infrastructures capable of hyper-volumetric DDoS attacks exceeding 1 Tb/s have emerged in increasing numbers. No such cases have yet been observed in Finland.
- Many botnets exploit poorly secured consumer devices, such as media devices or tablets purchased from low-cost online retailers.
- Botnets also compromise virtual machines hosted in cloud services. Botnets composed of such resources can be significantly more powerful.

12 kk

Cyber weather
in the past 12 months

	2025											2026
	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Data breaches and leaks	🌧	⛈	🌧	🌦	🌦	🌧	⛈	🌩	⛈	🌧	🌦	🌧
Malware	🌦	🌧	🌧	🌧	🌧	⛈	⛈	🌧	🌦	⛈	🌧	🌦
Vulnerabilities	🌦	🌧	🌧	🌧	🌧	⛈	⛈	🌧	🌦	⛈	🌧	⛈
Scams and phishing	🌧	🌦	🌧	🌦	🌦	🌧	🌧	🌦	🌦	🌦	🌧	⛈
Automation and IoT	🌧	☀	☀	⛈	🌧	☀	🌧	🌧	🌧	🌧	🌧	🌦
Network performance	🌦	🌦	🌦	🌦	☀	🌦	☀	🌧	🌧	🌧	⛈	🌦

Cyber weather forecast

The cyber weather forecast provides a summary based on previous observations and an indicative assessment of cyber threats and their likely developments in the coming months.

Cyber weather forecast

Cyber threats remain at a typical level

Phishing targeting user credentials and account breaches that have troubled organisations are likely to produce secondary effects. Criminals use compromised accounts to carry out invoice fraud, including CEO fraud schemes. In addition, further phishing messages are often sent from hijacked accounts.

Holiday seasons are repeatedly reflected in our account breach statistics: when staff return from leave to full inboxes, the risk of falling victim to phishing increases. The February–March winter holiday period may also lead to a rise in accommodation- and travel-themed phishing messages.

Vulnerabilities in network edge devices increase the attack surface for malicious actors. Exploiting such vulnerabilities may result in data breaches or attempted intrusions.

Organisational preparedness

- Awareness-raising and multi-factor authentication (MFA) alone are not sufficient to protect employees against advanced account takeover attempts, such as phishing campaigns using the AiTM technique.
- Organisations should implement advanced security features, including conditional access policies, risk-based authentication and continuous access evaluation.

Worrying

The volume and severity of cyber threats remain at a typical level.

However, the threat landscape can change rapidly — including in a negative direction.

The cyber weather forecast provides a summary based on previous observations and an indicative assessment of the cyber threat situation. It should not be used as the sole basis for preparedness; organisation-specific information and analysis must also be considered.