TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

August 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 cybersecurity.

Cyber weather can be:

 calm

 worrying

 serious

Overview of cyber weather in October 2026

Major international cyber incidents also brought storms to Finland

Critical vulnerabilities discovered in the PHP programming language were among the most significant cybersecurity incidents in October. PHP is widely used to power websites and online services around the world. Security measures taken by organisations caused widespread outages affecting online services.

In October, cyberattacks targeted refrigeration control systems in supermarkets across Europe. Similar attacks also spread to Finland in early November. The security of operational technology (OT) devices has been a prominent concern for some time, particularly following attacks on the energy and water supply sectors.

Large numbers of vulnerabilities continued to be disclosed.

Dark clouds gather as AI is increasingly used in scams

Reports received by the NCSC-FI indicate that video call scams involving criminals impersonating police officers or bank employees have become more common. Deepfake technology is suspected of being used in these scams. The aim is to obtain online banking credentials, payment card details and other personal data.

Scam messages impersonating hotels and other accommodation providers were also prominent in October. The messages used genuine booking details that may have been leaked from an accommodation provider or booking system.

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



October was European Cybersecurity Month. The EU campaign aims to raise cybersecurity awareness among individuals and organisations. The NCSC-FI participated in the campaign by sharing cybersecurity tips for everyone from a cybersecurity awareness network on social media.



Traficom introduced new requirements to make SMS scams more difficult to carry out. From 2 November 2026, telecommunications operators must replace the sender ID of a text message with a spam label or block the message if the sender has not obtained verified authorisation to use the sender ID.



The importance of securing IoT and OT devices has been a prominent topic, particularly in recent months. We published a comprehensive article outlining the principles of securing these devices and discussing recent cybersecurity incidents.

Hail shower of the month
Critical vulnerabilities in the PHP programming language

PHP vulnerabilities caused a significant international cybersecurity incident

Critical vulnerabilities allowing remote code execution were discovered in PHP, a programming language widely used to develop online services. By exploiting these vulnerabilities, an attacker may be able to execute commands of their choice on a vulnerable server and potentially take control of it.

The vulnerabilities were disclosed on 20 October, and security patches were released on 21 October. Following the disclosure, potentially millions of websites worldwide were temporarily taken offline. Attack methods exploiting vulnerabilities can be developed very quickly, particularly after the release of a software version that fixes them.

Significant scanning activity and exploitation attempts targeting the PHP vulnerabilities were observed. The first confirmed cases of successful exploitation were detected around the world soon afterwards.

The NCSC-FI is not aware of any cases of exploitation or intrusion involving these PHP vulnerabilities in Finland. However, measures taken to address the vulnerabilities caused outages affecting numerous services, as vulnerable services were shut down or access to them was restricted as a precaution.

The vulnerabilities constituted a major international cybersecurity incident, with an exceptionally wide range of potential impacts. PHP is used in numerous online services worldwide, meaning that the vulnerabilities could potentially affect a wide variety of organisations and service providers. The potential risk is further increased by the fact that PHP may also be used in third-party software and devices.

Cyber weather phenomena

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

Cyber weather
October 2026

1 mo.

Data breaches and leaks

The number of data breach reports increased significantly in October. WordPress vulnerabilities were exploited to distribute ClickFix content, highlighting the importance of security updates. The number of Microsoft 365 account breaches increased sharply.

Malware

During October, malware was observed being distributed through individual email attachments and compromised websites using the ClickFix technique, among other methods.

Vulnerabilities

Six vulnerability advisories were issued in October.

The number of vulnerabilities continued to rise, with more than 17,000 new CVE identifiers assigned during October, compared with 4,273 in October 2025.

Scams and phishing

The number of scams impersonating accommodation booking services, public authorities and banks increased.

Efforts to combat SMS scams were stepped up: unregistered sender names are now replaced with a spam label.

Automation and IoT

Cyberattacks targeting refrigeration equipment in Europe caused significant product losses and financial damage.

The attacks highlighted the risks posed by vulnerable remotely controlled devices, which apply to all systems accessible from the public internet.

Network performance

October was a typical month in terms of denial-of-service (DoS) attacks. DoS attacks were observed, occasionally causing limited disruptions to service availability.

Cyber weather
October 2026 1/2

1 mo.

Data breaches and leaks

- The number of reported data breaches increased significantly compared with September, although the month was otherwise fairly typical.
- Software vulnerabilities were extensively exploited in some of the reported data breaches. In most cases, WordPress vulnerabilities were exploited to add ClickFix content to websites. Organisations should prioritise updating their WordPress sites and managing vulnerabilities.
- The number of Microsoft 365 account breaches increased sharply in October. The highest number of incidents was reported by small organisations in the property and construction sectors.

Malware

- During the reporting period, malware and its distribution were observed particularly in connection with the ClickFix technique. For example, breaches of WordPress sites often resulted in malicious content being uploaded to compromised websites, which were then used to distribute malware.
- The NCSC-FI received a report of an incident in which a customer had provided an organisation with a USB stick containing malware. The malware was detected before it could cause any harm.

Vulnerabilities

- The PHP vulnerabilities CVE-2026-109618 and CVE-2026-109619 (PHP2Shell) attracted the most attention in October.
- By exploiting these vulnerabilities, an attacker may be able to remotely execute arbitrary commands on a server and take complete control of it.
- Several organisations, including Government ICT Centre Valtori, shut down their services before patches for the vulnerabilities were released.
- So far, no exploitation of these PHP vulnerabilities has been observed in Finland.

Cyber weather
October 2026 2/2

1 mo.

Scams and phishing

- October was European Cybersecurity Month. Public authorities, educational institutions and organisations shared practical tips for staying safe online through the *Nyt valppaana* network for promoting cybersecurity awareness. The network will continue providing cybersecurity advice in November.
- The number of scams impersonating accommodation booking services, public authorities and banks increased in October.
- Fortunately, efforts to combat SMS scams were also stepped up: unregistered sender names are now replaced with a spam label.

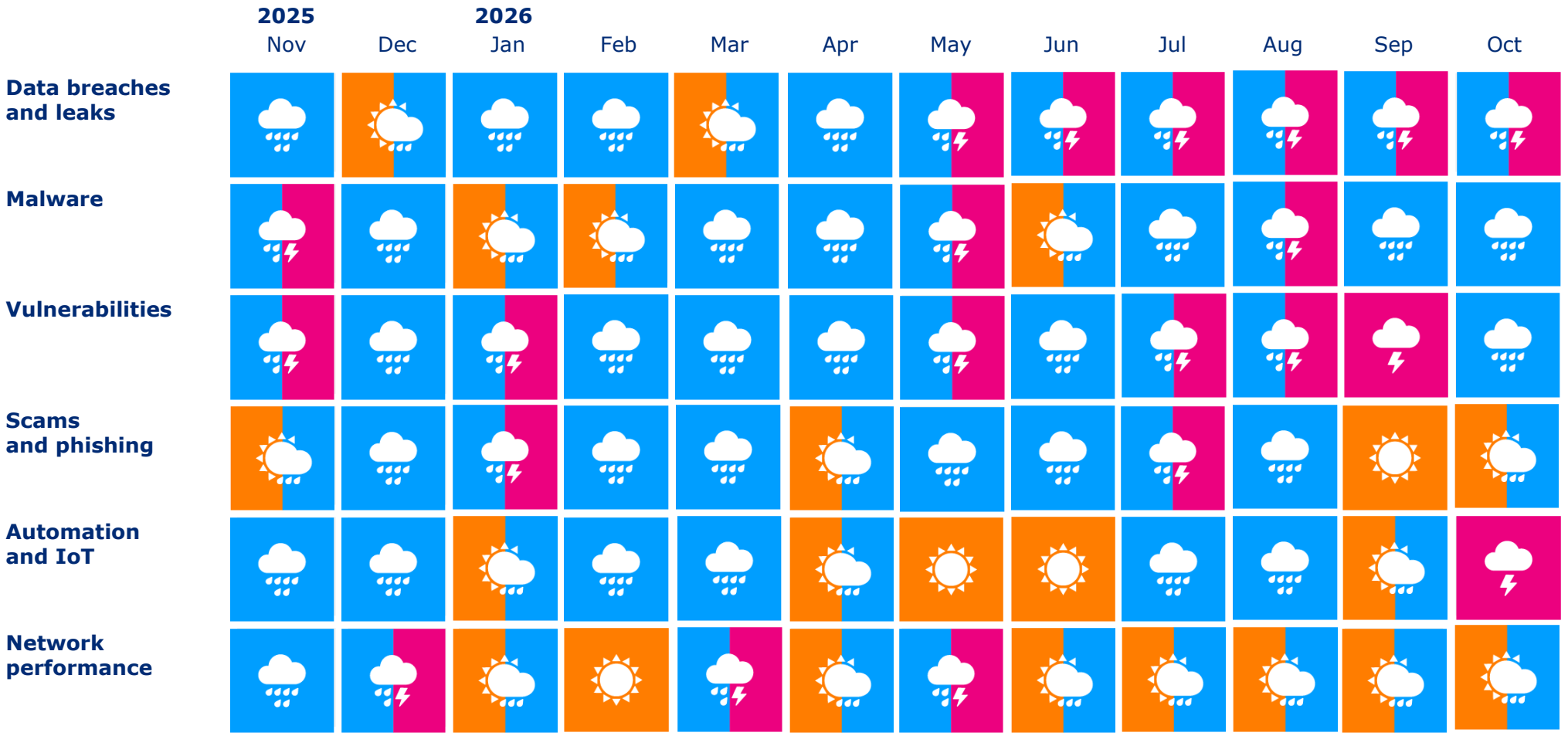
Automation and IoT

- Cyberattacks targeting refrigeration equipment in Europe demonstrated the risks posed by remote control systems accessible from the public internet. Attacks were also observed in Finland.
- France attributed the attacks on refrigeration equipment in the country to Iran. The perpetrators of the attacks in other countries are not yet known.
- These incidents highlight the importance of risk management and cybersecurity in systems that affect the physical world. IoT and OT devices should not be directly exposed to the public internet unless absolutely necessary.

Network performance

- Denial-of-service attacks can be carried out not only by generating large volumes of traffic but also by exploiting software vulnerabilities or weaknesses.
- The regulation on disturbances in telecommunications was updated and issued on 15 October. The regulation affects how telecommunications operators report disturbances to both consumers and Traficom. The regulation will enter into force on 1 January 2027.

Cyber weather
in the past 12 months



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.

1 mo.

Cyber weather forecast
Cyber threats remain at a typical level

The saying that cybersecurity knows no national borders became particularly evident to the public in October, and this is likely to remain the case. Cyber campaigns and incidents caused by critical vulnerabilities that affect multiple countries simultaneously are expected to continue.

Waves of Microsoft 365 account breaches are also likely to continue throughout the rest of the year.

Organisational preparedness

- Organisations should invest in user training to ensure that users can recognise Microsoft 365 credential phishing attempts and report them to IT support.
- Organisations should continue to be prepared to apply security updates rapidly, as critical vulnerabilities are being disclosed in quick succession.
- 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 are 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.