TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

May 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 Month 2026

May remained unsettled, largely due to vulnerabilities

May's cyber weather was mixed and at times unsettled. During the month, recurring and wide-ranging scam campaigns were observed, with criminals impersonating, among others, children, authorities, banks and service providers.

At the same time, phishing continued to evolve technically. Microsoft 365 accounts were targeted with AI-assisted phishing, making messages increasingly convincing. In April, we forecast that follow-on phishing campaigns would result from Microsoft 365 account breaches. This materialised, for example, in the form of device code phishing, which is more difficult to detect. In May, we also warned about the wave of instant messaging account takeovers that has continued throughout the year and provided guidance on how to protect against it. Several critical vulnerabilities were disclosed during the month, some of which were already being actively exploited.

Periods of sunshine in the cyber weather came from NCSC-FI's renewed Hyöky service, which was introduced for wider use, and from the launch of the FINMISP service, which enhances the sharing of technical cyber threat intelligence among organisations critical to security of supply and public authorities.

Information security does not take a summer holiday

During the summer holiday season, CEO fraud and other payment-related scams tend to increase as normal organisational routines slow down and key personnel are absent.

Risks are particularly elevated when responsibilities are handled by temporary replacements or summer employees who may not yet be familiar with organisational procedures. For this reason, effective onboarding and clear operating procedures play an important role in maintaining security.

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

Microsoft has launched one of the most important security updates of recent years: the renewal of Windows Secure Boot certificates. One of the main reasons for the change is that some Secure Boot certificates currently in use are reaching the end of their life cycle. Root certificates introduced in 2011 will begin to expire from summer 2026 onwards. In practice, the change affects almost all Windows devices manufactured after 2012. Microsoft estimates, however, that most modern Windows 11 devices will receive the updates automatically via Windows Update.

A new wave of Microsoft 365 phishing has been observed: an AI-assisted device code phishing campaign. The campaign targets both organisations and individual users. The aim of the attack is to gain unauthorised access to accounts and company resources. A data breach carried out using this new type of M365 device code phishing is not detected by Microsoft’s traditional phishing attack alerts. This gives attackers the opportunity to carry out invoice fraud, for example, without being noticed.

Organisations are therefore advised to use a query to check for device code breaches and to restrict the use of Device Code Flow through Conditional Access policies. Our website provides more information on how organisations and individuals can protect themselves against this phenomenon. The article also includes instructions for creating the search query.

Cyber weather phenomena

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

Cyber weather
May 2026

1 mo.

Data breaches and leaks

The number of data breaches increased by 24% compared with April. The rise is explained by the wave of Microsoft 365 account breaches. We received two ransomware reports. Serious impacts were avoided.

Malware

Several malware detections were reported to the NCSC-FI. Malware was distributed to organisations and private individuals as attachments to phishing messages, in connection with recruitment scams and through compromised websites.

Vulnerabilities

A large number of new vulnerabilities were also reported in May, and this trend is expected to continue for the remainder of the year.

Scams and phishing

"Hi Mum" scams were observed on Mother's Day. Scams are increasingly being created using AI tools.

CEO fraud tends to increase during the holiday season. Fraudsters attempt to deceive summer holiday replacements in the name of company executives.

Automation and IoT

The national Cybersecurity Act supplementing the EU Cyber Resilience Act (CRA) entered into force on Monday, 1 June 2026.

Network performance

Denial-of-service attacks did not cause significant disruptions in Finland.

Network service disruptions were more prominent in May.

Cyber weather
May 2026 1/2

1 mo.

Data breaches and leaks

- Vulnerabilities published in May led to data breaches in several organisations. However, serious impacts were avoided.
- After a quiet start to the year, we received ransomware reports. Organisations' preparedness has improved, and recovery from ransomware attacks is generally effective. In one case, the attack was detected so quickly that the attacker's activities could be monitored in real time and access to the organisation's environment was prevented.
- Several M365 account breaches occurred after victims inadvertently authorised an attacker's device using their own M365 credentials. The accounts were then used in invoice fraud attempts.

Malware

- During May, malware distribution and data leaks resulting from these infections were a significant nuisance.
- Trojans were successfully distributed to workstations through recruitment scams, resulting in workstation data being leaked to attackers.
- A supply chain attack targeting an international company enabled malicious software to be distributed in May to various organisations using the company's products and services.
- Malware was also distributed using the ClickFix technique through compromised websites.

Vulnerabilities

- In May, five vulnerability advisories were issued.
- The vulnerabilities affected Drupal Core (CVE-2026-9028), Cisco Catalyst SD-WAN (CVE-2026-20182), cPanel and WHM management software (CVE-2026-29201, CVE-2026-29202, CVE-2026-29203), Ivanti EPMM (CVE-2026-5786, CVE-2026-5787, CVE-2026-5788, CVE-2026-7821, CVE-2026-6973), and the User-ID Authentication Portal service in Palo Alto PAN-OS (CVE-2026-0300).
- Some of the vulnerabilities have been actively exploited.

Cyber weather
May 2026 2/2

1 mo.

Scams and phishing

- On Mother's Day in May, criminals attempted to make parents believe that their child had a new phone. The scam message was used to try to persuade the mother to send money.
- Traficom has also been used as a pretext for scams. Phishing messages refer to an unpaid fine becoming overdue and use this to harvest online banking credentials.
- As the summer holiday season approaches, CEO fraud is also becoming more common. Fraudsters attempt to trick summer holiday replacements into approving payments to criminal-controlled accounts by using messages forged in the name of company executives.

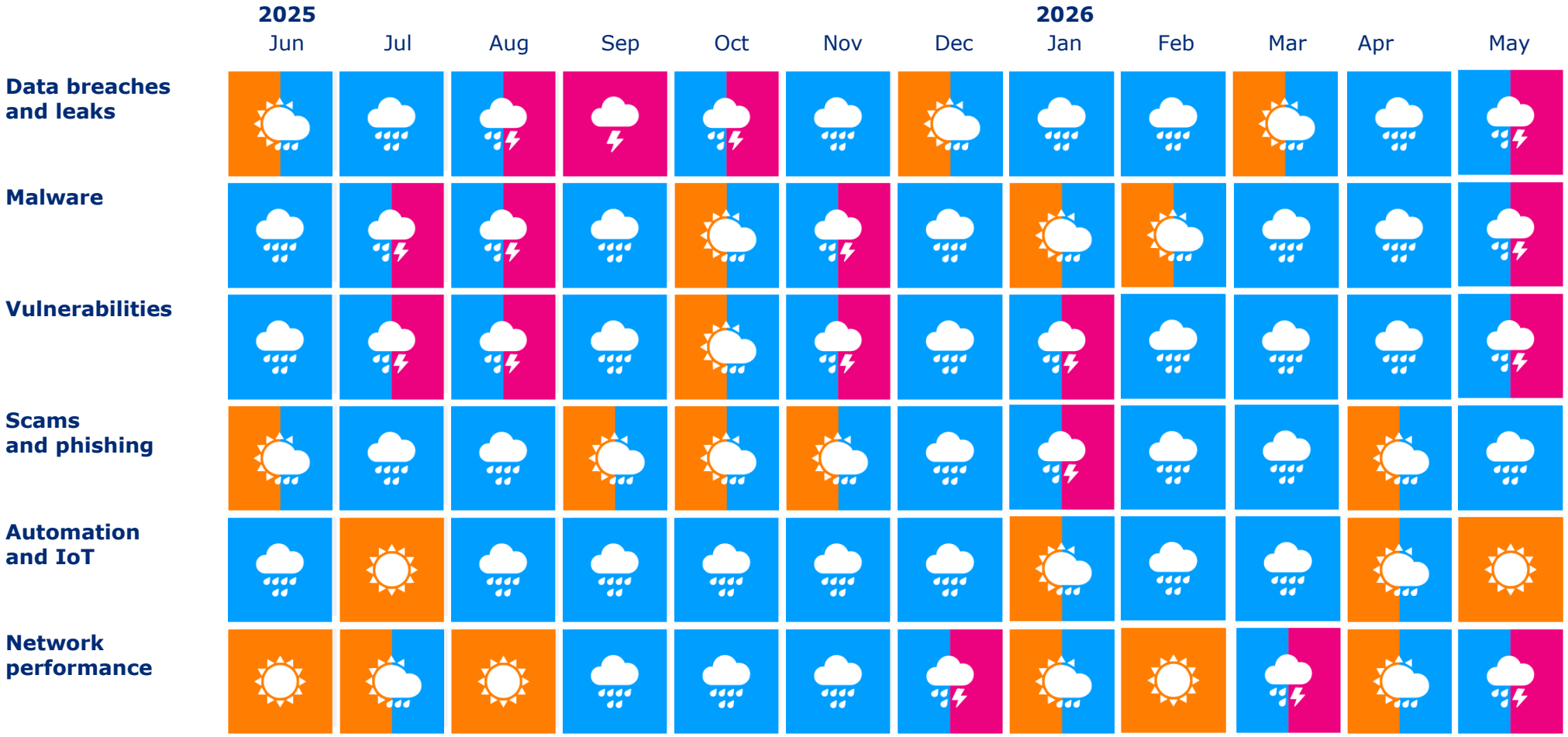
Automation and IoT

- The national Act on the cyber resilience of certain products and cybersecurity certification, which supplements the CRA, entered into force on 1 June 2026. The Act covers market surveillance, the notification of notified bodies and administrative consequences. It also supplements national regulation on EU cybersecurity certifications. The Finnish Transport and Communications Agency Traficom is centrally responsible for these tasks.
- The provisions concerning notified bodies will begin to apply on 11 June 2026. From that date, organisations may apply to Traficom for notification to carry out conformity assessment tasks under the CRA.

Network performance

- Denial-of-service attacks are a fact of everyday life on the internet, which is why services provided online must be protected. Although such attacks cannot be prevented entirely, they can be mitigated and their impact minimised.
- The number of serious network service disruptions was exceptionally high in May.

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.

Cyber weather forecast
Cyber threats remain at a typical level

No significant changes are expected in the cyber weather for June. Data breaches and vulnerabilities are likely to continue at their current level. The effects of the summer holiday season on cybersecurity are expected to become visible in June in the form of various scams, including CEO fraud and phishing campaigns related to travel and holiday arrangements.

Organisational preparedness

- Organisational preparedness and readiness must not depend on whether cybersecurity personnel are on holiday.
- Before leaving for holiday, you should ensure that the devices and applications you use are up to date and apply any necessary updates.

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.