TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyber weather

June 2025

Cyber weather June 2025

Data breaches and leaks 🌦

- June was relatively peaceful in terms of data breaches and leaks.
- Vulnerability scanning is active. Attackers are constantly looking for vulnerable devices or software that can be exploited for data breaches.
- Microsoft 365 phishing campaign targeting M365 email accounts was active. Stolen credentials enabled the sending of thousands of phishing messages.

Scams and phishing 🌦

- Online scams have increased alarmingly. The National Cyber Security Centre published guidelines for victims of scams. Don't struggle alone if you've been scammed!
- Scam calls are made in the name of banks, the police, or other authorities. In June, scammers have claimed to be calling from the National Cyber Security Centre.

Malware and vulnerabilities 🌧

- During June, increased activity of the BadBox 2.0 malware was observed, affecting devices running the Android operating system.
- In June, critical vulnerabilities were identified in NetScaler ADC & NetScaler Gateway products, as well as in Cisco ISE and Passive Identity Connector products.

Automation and IoT 🌧

- Android-based TVs, TV boxes, tablets, and other terminal devices have been taken out of service due to the BadBox 2.0 malware, which was installed during the manufacturing stage.
- BadBox 2.0 serves as a prime example of the importance of cybersecurity in the supply chains of IoT devices — in this case, particularly with regard to consumer electronics.

Network performance ☀

- In May, one disruption was detected in public communications networks.
- DoS attacks did not cause significant impacts in Finnish online services.

Spying 🌧

- The situation in the Middle East has an impact on cyber security both as hacktivism and cyber espionage.
- A threat actor publicly linked to North Korea continues its campaign targeting software developers, attempting to trick individuals into installing malware on their devices under the guise of, for example, a job-related test or a request for assistance.

NCSC-FI’s tips and recommendations for improving cyber security preparedness:

Cyber sector in transition webinar was arranged on 9 June. The webinar focused among other things on the development, opportunities, and security challenges of space and quantum technologies. A recording of the webinar is available on Traficom’s YouTube channel.

Virtually anyone can fall victim to an online scam or fraud, and such incidents can have a significant impact on a person’s finances or peace of mind. However, help and support are available from many sources. We published an Information Security Now! Article ”*Where to get help if you fall victim to an online scam?”.*

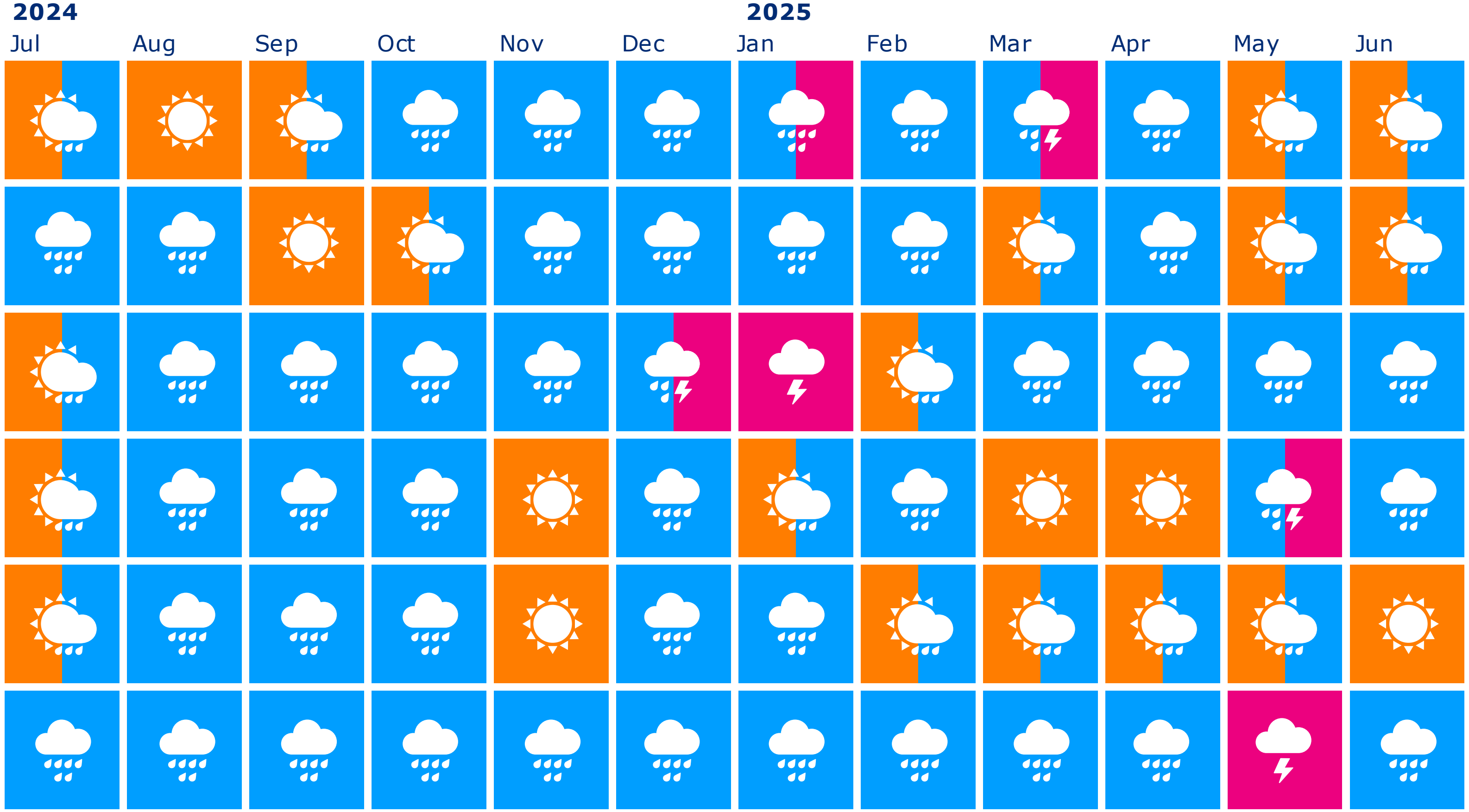
We also published two guidelines for improving Microsoft 365 environment concerning ’Admin Consent Workflow’ and ’Unified Audit Log’ functions. The Admin Consent Workflow allows for controlled granting of application permissions and reduces the risk of misuse, while the Unified Audit Log feature enhances visibility into user and administrator activities. These features help prevent account breaches, monitor file usage, and meet data protection and monitoring requirements.

Overview of cyber security in June

- The early summer has mostly brought mild cyber weather, and June was no exception to this trend. Themes typical of the summer season continued to be significant from a cyber security perspective:
  - Observed themes in June included banking, taxation, Suomi.fi, My Kanta and CEO-related scams. Mobile certificate phishing is still being identified.
  - NCSC's weekly review covered scams related to ETA and ESTA travel forms required for international travel which impose additional costs and may compromise data. In case of travel authorisation or visa, one should always use websites and instructions of the authority responsible for the processing of the authorisation.
- Malware caused threats especially for consumers when observations of BadBox 2.0 spread rapidly in Finland in mid-June. We published an Information Security Now! –article that provides a more in-depth look at the malware. Regarding other malware, the cyber weather during the month was considerably calmer.
- In England, a ransomware attack on a hospital was reported to have played a role in a patient's death due to delays in essential medical testing. The case is among the first where a cyber attack may have contributed to the loss of human life.
- New records were once again set in the field of distributed denial-of-service (DDoS) attacks, as Cloudflare reported a 7.3 Tbit/s attack that generated approximately 37.4 terabytes of traffic in just 45 seconds.

1 kk

Cyber security trends
in the past 12 months



	2024						2025					
	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Data breaches and leaks	🟧🟦 🌦	🟧 ☀	🟧🟦 🌦	🟦 🌧	🟦 🌧	🟦 🌧	🟦🟥 🌧	🟦 🌧	🟦🟥 ⛈	🟦 🌧	🟧🟦 🌦	🟧🟦 🌦
Scams and phishing	🟦 🌧	🟦 🌧	🟧 ☀	🟧🟦 🌦	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟧🟦 🌦	🟦 🌧	🟧🟦 🌦	🟧🟦 🌦
Malware and vulnerabilities	🟧🟦 🌦	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟦🟥 ⛈	🟥 🌩	🟧🟦 🌦	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧
Automation and IoT	🟧🟦 🌦	🟦 🌧	🟦 🌧	🟦 🌧	🟧 ☀	🟦 🌧	🟧🟦 🌦	🟦 🌧	🟧 ☀	🟧 ☀	🟦🟥 ⛈	🟦 🌧
Network performance	🟧🟦 🌦	🟦 🌧	🟦 🌧	🟦 🌧	🟧 ☀	🟦 🌧	🟦 🌧	🟧🟦 🌦	🟧🟦 🌦	🟧🟦 🌦	🟧🟦 🌦	🟧 ☀
Spying	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟦 🌧	🟥 🌩	🟦 🌧