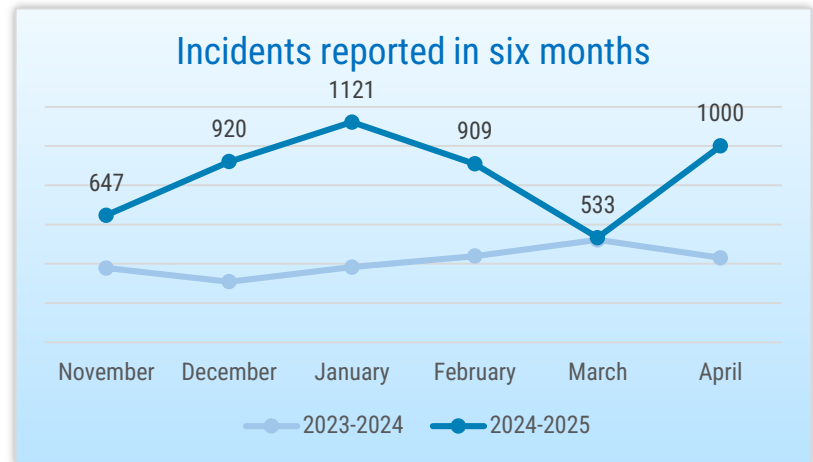




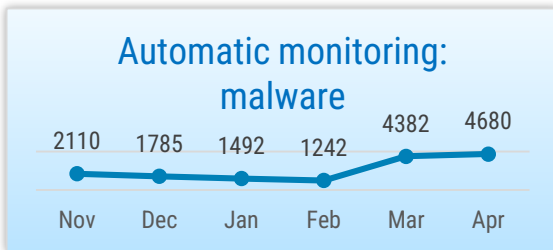
# SITUATION IN CYBERSPACE

APRIL 2025

- In April, **we recorded 1000 incidents with an impact**, which is a higher indicator than the average of the last six months.
- At the beginning of April, a large number **of denial-of-service attacks occurred in Estonia**. Fraud calls made posing as the Health Insurance Fund and Facebook Marketplace scams were also popular.
- We wrote on the RIA blog about **scam emails sent posing as the Police and Border Guard Board**. Schools once again have the opportunity to **order free educational materials** to help children recognise and avoid the dangers of using the internet.
- The party of the **Polish Prime Minister** was hit by a **cyber attack**. **Sensata Technologies**, a US technology company, fell victim to a **ransomware attack**. The British supermarket chain **Marks & Spencer** halted e-commerce orders for a few days due to a **cyber attack**.



Incidents reported to CERT-EE that had an impact on the confidentiality, integrity, or availability of data or information systems.



Devices in Estonian cyberspace infected with malware detected by automatic monitoring. CERT-EE notifies network owners of infections.



Phishing sites still account for the largest proportion of incidents recorded by CERT-EE.



# Situation in Estonian cyberspace

**A wave of denial-of-service attacks was carried out in Estonia on 3, 4, and 6 April.** The targeted websites were tartu.ee, pärnu.ee, kovtp.ee, emta.ee, omniva.ee, eesti.ee, tallinn.ee, evr.ee, elron.ee, rik.ee, ariregister.rik.ee, and e-estonia.com. This time, the attacks were technically more complex than usual, resulting in some websites experiencing short interruptions.

**On 7 April, between 10.49 a.m. and 6.56 p.m., sais.ee, the admission information system managed by the Ministry of Education and Research, was unavailable.** The failure was caused by a wrong file loaded into the system due to human error, which caused the memory to fill up.

On 16 April, between 11.32 a.m. and 12.42 p.m., **there were disruptions to the services of the Information Technology and Development Centre of the Ministry of the Interior (SMIT):** the border control information system PIKO, the authentication and procedure

information system UUSIS, software Apollo, the police tactical command database KILP, the file server, and the document management system Delta. As a result, automatic passport checks at Tallinn Airport were also disrupted. The incident was caused by a malfunction of the network equipment.

**In April, a new surge of fraud calls emerged, with fraudsters introducing themselves as Health Insurance Fund employees and asking for the PINs for documents.** The fraudsters stated that it is possible to apply for a discount on the increased fees for medical specialist visits from 1 April. They offered the possibility to book an appointment with an online consultant and asked the victims to identify themselves with Smart-ID. We recommend that you hang up all fraud calls immediately and avoid sharing your personal details or PINs.

**In April, people in Estonia once again fell victim to many Facebook Marketplace scams.** The scheme works as follows: the fraudster contacts a person selling an item on Facebook and claims to be interested in buying it. The buyer then informs the seller that they cannot collect the goods themselves and offers to use a courier service as a solution. The seller is then asked to pay a delivery fee or confirm the shipment of the parcel to verify the transaction and is led to a phishing site to enter their bank account details. In most cases, the phishing site looks very similar to the website of a courier service provider. Once the user has entered their details, as much money as possible will be taken from the card. Losses often run into thousands of euros; for example, in April, one fraud victim lost nearly 9,000 euros.



## Activities of the Estonian Information System Authority

**We wrote on the RIA [blog](#) about scam emails seemingly sent by the Police and Border Guard Board.** Such emails have been circulating in Estonian cyberspace for years, with no signs of slowing down. In April, they caused a lot of problems, so for educational purposes, we contacted the sender ourselves. People should not reply to these emails, as it usually leads to extortion attempts. The aim of such threats is to intimidate the victim into acting quickly, despite the grammar mistakes in and suspicious content of the email.

**On 17 April, another CyberMeetUp event took place at the Palo Alto Club.** This time, Martin Paas (Telia), Kalmer Päts (ByteLife), Ander Allas (Ministry of Defence), and Lauri Tankler and Tiina Pau (RIA) took to the stage. Participants could attend the event, watch it live online, or view it later on the RIA [website](#). The next CyberMeetUp will take place on 15 May.

**A new, 2025 version of the cyber test was made public in early April.** Like previously, the cyber test consists of two parts: a course on cyber hygiene and a practical test. In the course, we cover all of the most important topics related to cyber hygiene – password security, the spreading of malware, recognising phishing emails, using flash drives and other data media, secure remote working, using social media, and much more. The cyber test is free of charge for anyone who wants to take it and you can find out more about it [here](#).

**As we have seen a number of ransomware attacks significantly disrupting the work of businesses in recent months, we have updated the Remote Desktop Protocol or RDP [risk assessment](#).** The document outlines recommendations for securing the RDP connection and preventing ransomware attacks.

**This month, ETV aired the new episodes of the mini-series *IT-vaatlik*.** For example, there was an episode where RIA Prevention Manager Kaisa Vooremäe introduced Facebook Marketplace scams: how they work and how users can protect themselves. All episodes are available [here](#).

**Schools once again have the opportunity to order free educational materials to help children recognise and avoid the dangers of using the internet.** The materials were produced last year and proved extremely popular, with nearly 35,000 copies printed for 145 schools. RIA has therefore decided to issue a reprint and is waiting for orders from schools until 19 May. More information and the online order form can be found on the RIA [website](#).

**This summer, girls aged 13–16 can once again take part in the international cyber security camp *CyberWizards*,** for which you can find the registration form on our [website](#).



## International situation

**Polish Prime Minister Donald Tusk confirmed that his party was hit with a cyber attack, apparently aimed at influencing the presidential elections in May.** His Civic Platform candidate, Mayor of Warsaw Rafal Trzaskowski, is a presidential frontrunner and supports, among other things, even stronger ties with the European Union. Minister of Digital Affairs Krzysztof Gawkowski said that the relevant authorities are investigating the details of the incident, but it is likely that Russian and Belarusian hackers were behind the attack.

**The phishing campaign that started in Ukraine last November,** using information about members of the defence forces as decoys, is believed to be linked to the Russian state-backed group Gamaredon. An email with a malicious attachment is sent to the targets, the subject of which refers to the ongoing war and documents related to members of the defence forces. When the recipient opens the

attachment, spyware is installed on their device. Cyber security firm Cisco Talos has [analysed](#) the campaign and found a number of signs pointing to Gamaredon.

**Sensata Technologies, a US technology company, fell victim to a ransomware attack.** The attackers encrypted some of the systems and also stole data. According to the company, the attack disrupted production, delivery, receiving of components, and several support functions. Sensata manufactures sensors for cars, airplanes, and a range of industrial equipment, so supply chains were affected by the attack. In the fourth quarter of 2024, the company's revenue was over 900 million euros. No group has yet claimed responsibility for the attack but analysts speculate that Clop or LockBit may be involved.

**The British supermarket chain Marks & Spencer suspended online**

**orders for a few days due to a cyber attack,** and some stores were unable to accept card payments on site. Marks & Spencer has more than 1,400 stores in the UK and other countries. It is a publicly traded company, and due to the cyber attack, its shares fell by 5% in one day. Details of the attack have not been disclosed, but the company says it has informed the data protection authority and engaged private sector experts to resolve the incident.

**CISA confirmed that it has renewed its contract with MITRE, a non-profit organisation that actively manages the Critical Vulnerability Exploit (CVE) programme.** The statement was made after MITRE announced on 15 April that the continuation of the 25-year-old programme was in jeopardy due to the end of government funding.