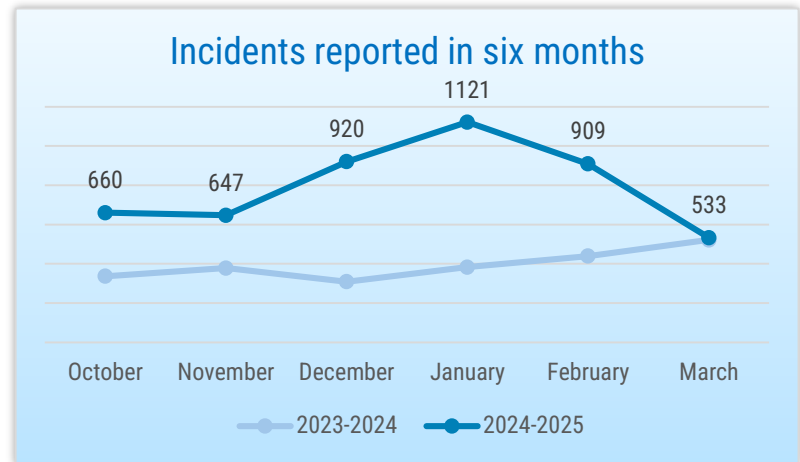




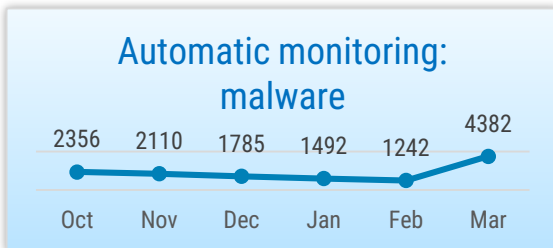
# SITUATION IN CYBERSPACE

MARCH 2025

- In February, **we recorded 533 incidents with an impact**, which is the lowest result in the last six months.
- The **Eesti.ee app was down** for more than a day. **Malicious emails** purporting to be sent on behalf of **law firms** reached the inboxes of many Estonian institutions and businesses.
- Gert Auväärt, Head of the Cyber Security Centre at RIA, participated in the **CYBERCAST podcast**. In the RIA blog, we wrote about the **security of email exchanges** and the hacking of Estonia’s public e-services.
- The US Secretary of Defence has ordered all cyber and **information operations towards Russia** to be put on hold. France’s Sorbonne University has been hit by a **ransomware** attack. **POLSA**, a Polish space agency, has announced that it has been hit by 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

## In March, several essential services experienced disruptions.

The Eesti.ee app was down for more than a day. From 1.54 p.m. on February 28 to 5.26 p.m. on March 1, the eesti.ee mobile application was down due to a configuration error. The outage lasted so long because of inadequate monitoring.

On 3 March, between 8.24 and 9.53 a.m., there was a disruption in the Active Directory (AD) login service at the Ministry of the Interior's Information Technology and Development Centre (SMIT). As a result, logging into the systems of the Ministry of the Interior, the Police and Border Guard Board, the Emergency Response Centre, and the Estonian Academy of Security Sciences could take minutes or fail completely. Outlook was also down during the outage and it was not possible to send emails. The outage was caused by an error in the AD controllers, which recovered after being restarted.

On 10 March, between 6.52 and 7.13 p.m., the use of Smart-ID was disrupted.

The failure was caused by a fault in the load balancer software, which was unable to service all requests. On the same day, between 5.21 and 5.47 p.m., there was a denial-of-service attack against the name servers of a commercial bank operating in the Baltic States. As a result, there were disruptions to online banking, the mobile app, and instant payments.

**Attacks against CERT-EE name servers continued.** Thanks to the safeguards in place, these attacks had no impact.

**In March, we were informed of two ransomware attacks, the exact circumstances of which are under investigation.** As ransomware often has serious consequences and can bring an organisation to a standstill, here are some ways to prevent it. Remote Desktop Protocol (RDP) connections should not be publicly available on the internet, but should be allowed from specified IP addresses. In addition, you should use a VPN (virtual private network) and two-factor authentication.

It is also important to regularly update your backups and keep them separate from the rest of the network, for example, on an external storage device.

**In March, malicious emails purporting to be sent on behalf of law firms reached the inboxes of many Estonian institutions and businesses.** The email reported copyright infringement for publishing video and audio files belonging to Estonian Television (ETV) on Facebook. The letter states that the evidence of the infringement is provided in the PDF file attached to the letter. In reality, there was a link inside the PDF file which, when opened, downloaded malware to the user's device. The emails were mostly signed with the names of well-known Estonian law firms, although a random Gmail address was used to send the email.



## Activities of the Estonian Information System Authority

**Gert Auväärt, Head of the Cyber Security Centre at RIA, recently spoke on an episode of [CYBERCAST](#) about how Estonia defends itself against cyber threats and what individuals can do to stay safer in the digital world.** The podcast also focused on the Cyber Security Yearbook and how cyber security affects every person and business.

**Joonas Heiter, Director General of RIA, gave an [interview](#) to the Digigeenius portal, explaining the creation of the new command centre and the reorganisation of the current CERT-EE monitoring team.** The entire change will be implemented with existing resources, without requesting an additional budget. This will include a thorough review of operational processes and an overhaul of the monitoring logic. The RIA command centre is expected to be operational in the first half of 2025.

**On 20 March, the monthly CyberMeetUp took place at the Palo Alto club.** On this

occasion, presentations were given by Rain Nõmmsalu (CybExer Technologies), Jack Shis (NATO CCDCOE), Jesper Olsen (Palo Alto Networks), and Teoh Chun Ping (Government Technology Agency of Singapore). Anyone who wishes to can either come to the event, watch it live online, or check it later on [the website](#) of RIA. The next CyberMeetUp will take place on 17 April.

**We have published recommendations for organisations to ensure the security and trustworthiness of their email communications on the [blog](#) of RIA.** Many fraudulent schemes use fake emails or phishing emails sent on behalf of an organisation to its partners. In this blog, we discuss how to properly set up your email and name server to minimise the risk of email spoofing.

**We recently published a post on the [RIA blog](#) about the surge in fraudulent calls over the past few months, many of which have been impersonating Omniva.** The scammers claimed that they were couriers and needed to deliver a parcel.

To do this, the victim was asked to use their Smart-ID account to confirm either the arrival of the parcel or a declaration from the tax office.

**We also [wrote](#) about phishing attempts impersonating Estonian government's e-services.** People are invited to these pages mainly through text messages containing various excuses for the recipient to click on the accompanying link. On the RIA blog, we took a closer look at phishing scam attempts involving text messages impersonating the Estonian Transport Board, and shared tips on how to avoid falling victim to such fraud.

**In March, the national television aired new episodes of its [IT-vaatlik](#) (IT-conscious) series, where we talked about PIN codes and phishing through text messaging.** All the episodes that have been broadcast can be viewed on [Jupiter](#).



# International situation

**US Defence Secretary Pete Hegseth has ordered the US Cyber Command to suspend all cyber and information operations towards Russia, in the context of Trump's aim to reach an agreement with Putin to end the war in Ukraine.** While this practice is not uncommon for high-level negotiations, the US approach to Russia and the U-turn in foreign policy has been striking to many observers. The suspension does not apply to cyber intelligence or signal intelligence. At the same time, threat analysts at the US cybersecurity agency CISA were instructed to focus on other targets rather than the Russian threat, and in a recent speech on cyber threats at the UN by a senior US State Department official, it was notable that Russia was no longer mentioned as a cyber threat alongside China and Iran.

**The Sorbonne University in France was hit by a ransomware attack claimed by a ransomware group called Funksec.** The type of ransomware used in the attack is believed by experts to be the first ransomware written with the help of

creative artificial intelligence, and the group Funksec, which emerged just a few months ago, stands out for its use of this new method. The range of Funksec's targets has been relatively wide, covering the government and defence sectors as well as financial institutions, education and technology. The group has had victims in the US, India, Spain, and Mongolia.

**The Polish Space Agency POLSA has reported a cyberattack and the disconnection of their information system from the network.** There is no official information on the nature of the attack, but according to one space agency employee, their internal email environment was compromised, among other things. According to Krzysztof Gawkowski, Poland's Minister for Digitalisation, an investigation has been launched and the country is doing its best to identify the intruder.

**The Danish Cybersecurity Agency has published a threat assessment, according to which the threat of cyber**

**espionage to European telecom companies has increased.** The risk of cyber-attacks against the Danish telecoms sector has been upgraded to 'high', with the highest risk of ransomware and cybercrime attacks.

**The UK's Data Protection Authority has fined Advanced Computer Software Group €3.6 million for a data breach.** The data was stolen from the company in a ransomware attack in 2022 by the group LockBit. Advanced Computer Software Group provides services to the National Health Service and other healthcare providers, among others, and the attack resulted in the leak of data on around 80,000 people, including the exact addresses of around 900 home care patients and instructions on how to get into their homes.