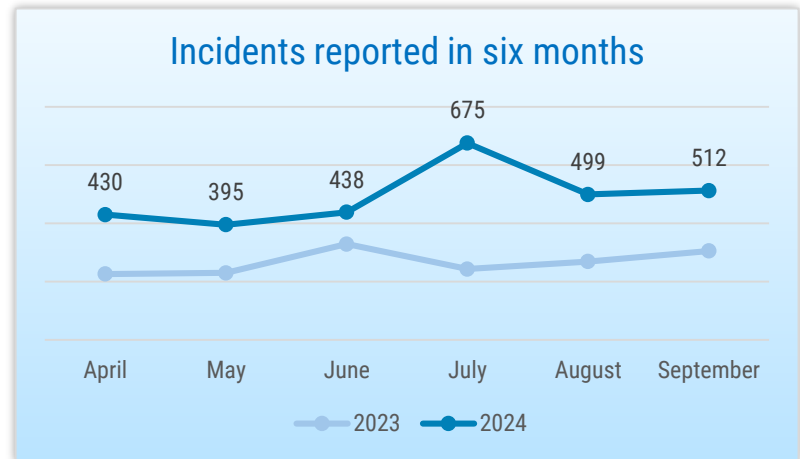




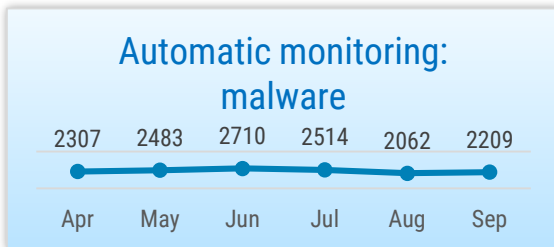
SITUATION IN CYBERSPACE

SEPTEMBER 2024

- In September, we recorded **512 incidents with an impact**, which is slightly above the average for the last six months.
- In September, **several essential services were disrupted**; for example, Telia voice communication and Swedbank services experienced failures. We saw a spread of **phishing emails sent posing as the bank LHV**.
- We are **organising cybersecurity workshops for adults**. We published new instructional materials for children and parents in Estonian.
- Estonia along with other countries published **a joint statement** to attribute cyber attacks to the Russian military intelligence. The car rental company **Avis fell victim 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

In September, several essential services experienced disruptions. At 10.56 a.m. on 5 September, calls in the Telia network started to fail. All across Estonia, it was impossible to make calls to numbers outside the Telia network; the failure impacted both landline and mobile phone calls. By 12.28 p.m., voice communication was largely restored, but some clients could have experienced problems afterwards as well. For about an hour, placing calls to the emergency number 112 was also disrupted. The failure was caused by a software error in the voice communication system.

From 6.58 a.m. until 8.44 a.m. on 16 September, there was a large-scale interruption in the operation of websites. For nearly two hours, several important websites would not open, such as the tara.ria.ee state authentication service. Over 200 various websites were impacted. The problem was caused by a technical error in the CloudFlare data centre

providing protection against denial-of-service attacks.

In the early hours of 17 September, at 4.35 a.m., the core network of the IT and Development Centre of the Ministry of the Interior (SMIT) experienced data communication failures during maintenance, leading to interruptions in services provided by SMIT, including in the emergency notification system used by the Emergency Response Centre for processing calls. The Emergency Response Centre was able to return to its regular operations only at around 8 a.m., whereas most of the SMIT's services were restored sooner.

On 26 September, from 3.28 p.m. until 7.09 p.m. and from 8.05 p.m. until 9.02 p.m., card payments and the operation of the internet bank of Swedbank were interrupted. On the same day, the services of another bank were also disrupted. The reason for the failures is currently unknown.

In September, phishing emails started to spread, seemingly sent by the bank LHV, asking users to update their information. The emails were sent from a suspicious email address not belonging to LHV, and they contained a link directing users to enter their bank card details. Unfortunately, many people were fooled by the email and CERT-EE received several reports of the loss of large amounts of money. In some cases, the loss exceeded 10,000 euros. We would like to remind you that a bank does not send such emails or ask customers to update their information through an unknown link. When a bank needs to update their information, they send a notification through the internet bank and the data is also renewed in the same environment.



Activities of the Estonian Information System Authority

Starting from the end of September, we are going to hold 25 free workshops for adults, teaching how to recognise online threats and to protect computers and smart devices better. The workshops are primarily meant for middle-aged and older people (55+), but everyone who is interested is welcome. For instance, participants learn how to recognise phishing pages, fraudulent phone calls, and other criminal schemes. The workshops last about two hours and take place all across Estonia in local libraries and social establishments from the end of September until the beginning of November. Details about the times and locations of the workshops are available on the [website of RIA](#).

On 30 September, the first episode of the IT-vaatlik TV programme was aired. The first episode focused on phishing and scams and viewers learned about how scammers acquire our data and what they do with it. The show is going to air over the course of

26 weeks on ETV and it will discuss various essential cybersecurity topics. During the episodes, we will review how to use the internet and social media safely. The episodes are available on the [Jupiter](#) streaming platform and is an important part of the [awareness campaign](#) that RIA organises every autumn, lasting until the end of October.

We published new instructional materials in Estonian for children of primary school age and their parents on the website of RIA, helping to identify and avoid hazards related to the use of the internet. RIA's [workbook](#) is suitable for children aged 7–11 and it introduces topics related to the safety of the internet and smart devices in a manner that is clear and appealing for children, using crosswords, exercises, and games. [Auxiliary materials](#) for adults focus on protecting children and teaching them about online threats.

The cyber test is now available in English! The cyber test is an online training environment created by RIA, covering all essential cyber hygiene topics and helping to maintain the level of cybersecurity awareness of staff. We welcome all organisations and companies to join the cyber test. If you would like to take the course in English, please send an email to kybertest@kybertest.ee.

In September, we launched nine new supervisory proceedings to check compliance with the requirements established in accordance with the Cybersecurity Act. The purpose of the proceedings is to verify compliance with organisational, physical, and IT security measures by a company or a public authority. The functioning of information security and risk management processes and the implementation of E-ITS security measures by state authorities were under particular scrutiny.



International situation

The US, the UK, the Netherlands, Czechia, Estonia, Latvia, Canada, Australia, Ukraine, and Germany issued a [joint statement](#) on 5 September, attributing cyber attacks committed against several countries over the last few years to unit 29155 of the Russian military intelligence (GRU). In the opinion of the cyber authorities of these countries, the objective of the unit is cyber espionage, sabotage, and causing reputational damage. The unit committed a number of cyber attacks against Estonian public authorities in 2020 (including data theft); the unit is also linked to the attacks against Ukraine in 2022, which used the WhisperGate malware that destroys data.

The car rental company Avis fell [victim](#) to a cyber attack in the beginning of August, and by now, it has become clear that the personal data of at least 300,000 individuals was leaked, including credit card details and driving licence numbers. The leak

mainly concerns the US customers of the company, who have been notified. Considering the number of customers of Avis and the level of sensitivity of the data they store, the incident has sparked outrage regarding the insufficient cybersecurity measures of the company.

In September, Ukrainian hackers [carried out](#) an attack against a public authority called Osnovanie that certifies digital signatures in Russia.

The attackers defaced the website of the authority, leaving the following message: 'Your certificates are in safe hands; the proceeds from the sale are used to support the Ukrainian defence forces.' According to Osnovanie, the attackers only managed to deface the website, while the infrastructure related to digital signatures was unharmed. However, the site was still down several days later, and according to Russian customers, digital signature services were unavailable. Ukrainian military intelligence in cooperation with

the BO Team hacker group took responsibility for the attack, and according to them, they managed to destroy some of the databases and also steal some of the data. According to Alexey Senchenkov, the Commercial Director of Osnovanie, servers located in the US, the Netherlands, and Estonia were used in the attack.

As a result of a [joint operation](#) of Europol, Eurojust, and nine countries, an encrypted communication environment called Ghost was shut down. It was used by organised criminal groups all across the world. The platform was favoured by the criminals because it allowed anonymous use, offered several encryption methods, and included a service which deleted sent messages from the device of the recipient after a certain time. As a result of the operation, 51 people were arrested, mostly in Australia and Ireland.