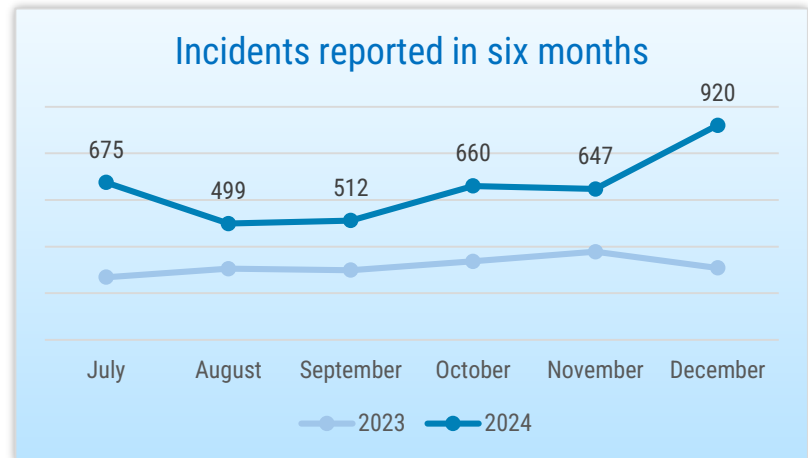




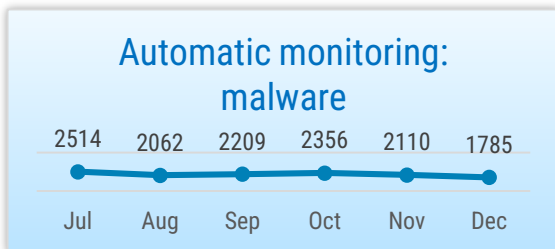
# SITUATION IN CYBERSPACE

DECEMBER 2024

- In December, **we recorded 920 incidents with an impact**, which is the highest result in the last six months. The majority of the incidents registered involved phishing sites.
- In December, an education sector company was hit by a **ransomware attack** and, at one state authority, the accounts of **previous employees had remained active**. Phishing attempts launched posing as LHV also continued in December.
- We published the new **'IT-vaatlik' prevention portal** and the new **eesti.ee mobile app**.
- The Ministry of Justice of Ukraine **fell victim to an extensive cyber attack**, which resulted in several public services becoming unavailable. The United States are planning to ban the **routers of the Chinese manufacturer TP-Link** due to security risks.



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

### **We registered the highest number of incidents last year in December.**

On 2 December, a company operating in the education sector fell victim to a ransomware attack. In the course of the attack, the attacker encrypted the data of the company in the Amazon cloud environment and demanded a ransom for the restoration of the data. The data in question was not personal data or business-critical data and the company accepted the loss thereof. The attack was possible due to an account with excessive rights.

In the early morning of 9 December, it was not possible to buy tickets in the city buses in Tartu. The electronic displays in front and on the side of the buses indicating the number of the line and the information screens at the bus stops were also not working. The interruption was caused by the systems of Ridango, the company providing the service to the public transport system of Tartu, running out

of disc space. The issues were eliminated at 10.30 in the morning.

Between 2.07 and 3.09 p.m. on 16 December, it was not possible to use Smart-ID authentication or signature. This was caused by a technical failure after executing a scheduled change.

In November, CERT-EE was notified that several dozens of employees of one state authority who had left their positions still had their official email addresses, which they could also still access. Accounts with administrator rights of some of the former employees were also still active. The impact and circumstances of the incident are being investigated.

**Various different incidents of fraud also continued in December.** We were again notified of many cases of people falling victim to phishing emails from LHV. In the emails, the recipients are asked to update their details and it appears as if they are accessing the

website of the bank when they attempt to do so, but the fraudsters have actually created an environment very similar to that of the bank. We would like to remind people once again that banks never ask anyone to provide their data by email or to log in to suspicious domains.

**We were also notified of a case where a child opened a link through a QR code on TikTok,** which ended up causing financial loss to the family. After scanning the QR code, a seemingly reliable website designed as a smartphone game opened for the user, where they were asked to confirm their wish to receive free extras for the game. After pushing the button, a huge number of messages were sent from the phone of the child to foreign phone numbers. More than 160 messages were sent within a few minutes, but the financial loss was fortunately not very significant. We advise to approach any links in QR codes very attentively and refrain from opening them in the case of any doubts.



## Activities of the Estonian Information System Authority

**A large-scale training took place on the initiative of RIA at the end of November, which involved practising the cooperation between national IT houses, other authorities, and the cyber reserve in responding to crisis situations.** According to the scenario of the training, anomalies were found in the information system of the justice sector, as a result of which the release of prisoners was temporarily suspended. Later, it turned out that there had been a cyber attack and highly sensitive data had been leaked. Among others, the technical experts of the cyber reserve managed by RIA were asked to help examine the reasons and restore services as quickly as possible. Public authorities also had to deal with countering extensively circulating misinformation. Therefore, the public relations specialists of several state authorities and the reserve members of the government communication centre were also involved in the training.

**In the beginning of December, the CyberBazaar 2024 innovation forum in Riga took place,** which was organised as a cooperation of the national cyber security centres of Estonia, Latvia, and Lithuania. There were presentations on three thematic stages: technology, science, and business development. In total, almost fifty specialists from the Baltic countries and further away spoke at the event. Within the framework of the forum, a hackathon was organised for the students at the University of Latvia, where the participants were competing in three categories: cyber security at the government level, cyber innovation, and increasing cyber awareness.

**The updated 'IT-vaatlik' prevention portal was launched on 11 December:** the appearance, structures, and content of the online environment were all given a makeover. In addition to the thoroughly updated instructions for private individuals, the portal also

includes a lot of other interesting material, such as a brief course on cyber defence, training videos, and our exciting radio and television shows. An important addition to the website is the 'Common scams' section, which introduces the most popular fraudulent schemes in Estonia to enable people to recognise them and prevent damage. Go and get acquainted with the updated [IT-vaatlik](#) environment.

**In the beginning of December, RIA published the new eesti.ee smartphone app, which brings public services straight into the pocket of the user.** The new app helps everyone to communicate with the state conveniently and securely – use public services, get acquainted with their data, and use private sector services in the future. There are almost fifty services in use already, with more to be added in the future.



## International situation

**The Romanian constitutional court ruled out the results of the first round of the presidential elections**, as, according to the intelligence service of the country, Russia had [organised](#) a coordinated campaign on TikTok in support of the far-right candidate Calin Georgescu. Georgescu, who had been relatively unknown so far, won the first round and promised, among other things, to end Romanian support for Ukraine. The report of the Romanian intelligence service also reveals that more than 85,000 cyber attacks were made against the election infrastructure. The attacks served different purposes: gaining access to the infrastructure and compromising it, amendment of the information related to the elections, and reducing accessibility.

**An Iranian threat is targeting the SCADA industrial equipment in the United States and Israel.** Experts of the cyber security company Claroty issued a special [report](#) about the malware

IOCONTROL targeting the Internet of Things (IoT) and industrial equipment. This malware is being used by the group CyberAv3ngers, which has Iranian connections, to target various different domestic and industrial devices in the United States and Israel, including security cameras, routers, firewalls, industrial automation control panels, etc. Petrol station equipment is also being targeted and, according to the group, they have managed to compromise 200 petrol stations in the United States and Israel over the past year.

**The databases of the Ukrainian Ministry of Justice were hit by an extensive cyber attack**, as a result of which, several public services (filing marriage applications, issuing birth certificates, registration of vehicles, etc.) remained unavailable for approximately two weeks. Several dozen services of the Diia app also had to be closed due to the attack, as it could not connect to the databases

required. When publishing details of the attack, the Ukrainian government reported that no data had been leaked or deleted, based on the initial assessment. A hacker group associated with the Russian military intelligence is believed to be behind the attack, which is the biggest recent attack against the critical databases of Ukraine.

**The United States is planning to ban the routers of the Chinese manufacturer TP-Link**, which are being linked to cyber attacks by Chinese hackers due to security risks, next year. According to analysts, the plan to ban TP-Link is primarily based on the concern about the large, approximately 65% market share of the routers of TP-Link among small businesses and private users, as well as the risks related to the connections of TP-Link with the Chinese government, which may materialise in the future.