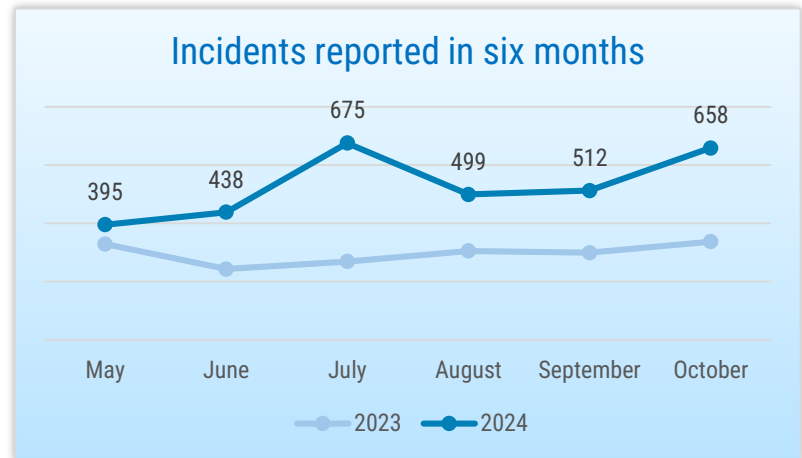




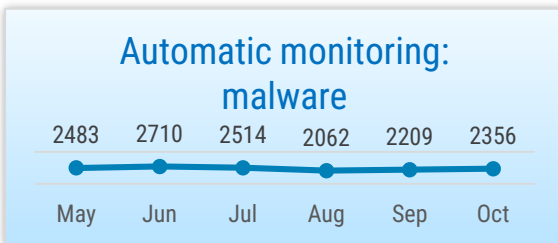
SITUATION IN CYBERSPACE

OCTOBER 2024

- In October, we recorded **658 incidents with an impact**, which is slightly above the average for the last six months.
- At the beginning of the month, the email addresses of some people who had applied to test the eesti.ee application **were leaked**. An unknown person **entered the file sharing server** of the Estonian Public Broadcasting (ERR).
- October is the international cybersecurity awareness month and we **organised an awareness campaign to prevent cyber threats**.
- French news agency Agence France-Presse (AFP), major water company American Water Works, and Iranian public sector organisations **fell under cyber attacks**.



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

Although October has been the month of cyber security for years, it did not unfortunately pass without incidents.

On 2 October between 9.49 a.m. and 2.55 p.m., the automatic border control system, i.e. the ABC-gates used for the verification of documents, were not working. The failure disrupted work at Tallinn Airport and the Narva and Saatse border crossing points. The cause of the incident is unknown but is not currently suspected to be an attack.

On 4 October, the email addresses of 350 people who had volunteered to test the eesti.ee application were leaked. A development partner of RIA inadvertently sent an email where all email recipients were visible due to human error. The people affected have been notified of the incident.

In the evening of 19 October, an unknown person entered the FTP server of the Estonian Public Broadcasting, which is used to

exchange files with cooperation partners. The person deleted the files in the server and uploaded new ones, some containing malware. The account that was compromised had been protected by a weak password. Fortunately, it was possible to recover the deleted files, but in the light of the incident, we recommend that you check your password policies and implement two-step verification wherever possible.

Starting on 29 October, the payment system at Krooning petrol stations experienced disruptions, resulting in funds being reserved from customer accounts in amounts larger than the actual payments required, with the excess amounts not being released afterward. Payment services for the petrol station chain are provided by the Finnish company Nets Finland, which is actively working to resolve the issue. Krooning has promised to return the additional reserved amounts to its customers as soon as possible.

In October, many people in Estonia lost money to fraudsters.

Different tactics were used, but the most common were phishing messages on behalf of postal service providers. For example, emails and text messages sent on behalf of different courier companies (DPD, DHL) were spread, asking people to renew their address or pay a fee. Several people also fell victim to a Facebook Marketplace scam. The scam works as follows: the fraudster contacts a seller on Facebook and claims they wish to purchase an item. The buyer then says that they are unable to collect the item in person and offers using a courier service instead. The seller is advised that they must pay a delivery fee or ensure the parcel to confirm the transaction and is directed to a phishing page to enter their bank card details. After that, at least several hundred euros are deducted from the account, but the amounts may often reach thousands of euros.



Activities of the Estonian Information System Authority

RIA's annual conference was held on 9 October and the topics covered included artificial intelligence, the future of digital identity (eID), implementing the E-ITS standard, the situation in cyberspace, Estonia's new cybersecurity strategy, the legal space, and changes related to the NIS2 directive. The speakers included staff members of RIA as well as our excellent cooperation partners. A couple hundred people attended the event in person and about the same number consistently followed the event online. The recording of the conference is available [here](#).

The first RIA CyberMeetUp of the season was held on 17 October. After the opening speech by the director general, five of the most successful startups of the cyber incubator introduced their ideas and finally, information was provided about the cyber forum CyberBazaar taking place at the beginning of December. The recording of the event is available [here](#).

Until spring, the TV channel ETV will air short programmes on cybersecurity titled *It-vaatlik* on Monday evenings. The programmes in October covered phishing pages, the Internet of things, malware, and passwords. The programmes can be re-watched on [Jupiter](#).

October is the cybersecurity month and we have organised an awareness campaign on preventing cyber threats.

Recent survey results show that most people in Estonia follow at least some recommendations for safe internet practices, while about ten percent do not follow any. On 3 October, Kaisa Vooremäe, Prevention Manager at RIA, discussed fraud schemes on the Booking.com website during [StarFM's](#) morning programme and shared tips for preventing internet fraud on [Radio Kuku](#). Please also listen to the *Pere ja kodu* magazine's [podcast](#) where we shared advice on cyber security for children and their parents.

In the [blog](#) of RIA, we spoke about the secure management of a company's social media. As an ever-increasing share of advertising budgets is allocated to social media channels to enhance company visibility, interest from cybercriminals in this area has also grown. The [blog](#) also covered Booking.com frauds, including how to avoid them and RIA's advice for people.

In October and November, we are organising E-ITS inclusion seminars in Tartu and Tallinn. At the [seminars](#), we share practical advice and recommendations with the implementers of the E-ITS to make it easier to understand the content and implementation of the standard.

In September and October, we held practical cybersecurity trainings for ICT teachers. The two-day training courses were organised in Tallinn, Tartu, and Pärnu with a total of nearly seventy teachers participating.



International situation

In early October, the French news agency Agence France-Presse (AFP) **announced** that they had suffered a **cyber attack on 27 September**. The incident had an impact on AFP's IT-systems and content delivery to its clients. AFP is working with France's cybersecurity agency (ANSSI) to specify the circumstances of the attack.

At the beginning of the month, one of the biggest water utilities in the U.S., the American Water Works, which supplies water to about fourteen million people in fourteen states, also **suffered** a cyber attack. The attack did not affect water supply or water quality but disrupted its billing system and client portal. No one has taken accountability for the attack yet. The water sector has been under the special attention of the U.S. government due to increasing attacks and deficient levels of cybersecurity.

On 12 October, Iran's public sector

establishments as well as critical sectors, such as nuclear facilities, fuel transportation, and ports, were hit by a heavy cyber attack. However, a former high official of Iran's Supreme Council of Cyberspace has said that sensitive information was stolen during the attacks. It is speculated that the attacks may have been the response of Israel to Iran's missile barrage on 1 October.

Ukraine's ministry of defence established a separate operational cybersecurity department CERT (Computer Emergency Response Team) for the defence of the state's defence force and military networks. Prior to this, the ministry had a dedicated team of cybersecurity professionals, but establishing a separate structural unit will expand its responsibilities and will help to further improve cybersecurity, including against cyberattacks from Russia. The new unit will also cooperate with NATO states.

In mid-October, two Russian hacktivist groups **organised a denial-of-service attack campaign against Japan's government organisations and logistics companies**. The attack came in response to Japan's recent decision to significantly increase its defence costs and to partake in military exercises with U.S. and other allies. The **report** of the cyber enterprise Netscout indicates that a total of 2,000 daily denial-of-service attacks were made against Japan's networks.

According to Microsoft's recent report, Russia, China, and Iran are increasingly cooperating with criminal groups to conduct their cyber operations. For example, in June, criminals managed to break into dozens of devices used by Ukraine's defence force staff and collect information relevant to the Russian government. Microsoft evaluates that the line between organised crime and the activity of nation-state actors is becoming increasingly blurred.