



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY



Cybersecurity quick guide for companies

2025

Contents

1	Strong companies create a stronger society	3
1.1	The responsibility lies with the head of the company	3
2	Determine the company's security needs.....	4
3	Know what hardware and software you are using.....	4
3.1	Hardware inventory	5
3.2	Software inventory.....	5
3.3	Consider implementing central device management.....	5
3.4	Establish rules for using personal devices in the working environment	6
3.5	Assess the implications of using cloud services	6
3.6	Use new technologies safely.....	8
4	Protect your assets	9
4.1	Give access rights reasonably	9
4.2	Update software regularly	10
4.3	Organise the protection of your company's computer network and its users	11
4.4	Prevent access to data in lost or stolen devices	11
4.5	Ensure the physical protection of data and devices	12
5	Protect your employees	13
5.1	Create a secure password policy	13
5.2	Use multi-factor authentication.....	13
5.3	Simplify the use of passwords.....	14
6	Learn to recognise attacks.....	14
6.1	Raise employee awareness	14
6.2	Train your employees.....	15
6.3	Regularly check your employees' knowledge	15
7	Prepare for incidents and learn to recover	16
7.1	Be prepared with a clear plan of action in the event of an incident	16
7.2	Create a recovery plan.....	16
7.3	Have a clear overview of what is happening in your systems	17
7.4	Ensure backup operation and verification.....	17
7.5	Perform recovery testing	18
8	Protect your brand.....	18
8.1	Acknowledge potential risks.....	18
8.2	Protect the company against threats	19
9	Pay attention to the supply chain.....	22

1 Strong companies create a stronger society

The Estonian Cybersecurity Act establishes cybersecurity requirements for companies and institutions whose activities are critical – public authorities, ports, energy companies, telecommunications operators, etc. At the same time, the cybersecurity of Estonian people depends on how securely all other, smaller companies and institutions, on which similar requirements have not been imposed, are able to protect themselves and their customers (their data). Hiring information security managers or teams may be out of reach for them, and cybersecurity standards may seem so extensive and resource-intensive that it does not seem commercially reasonable to implement them.

This quick guide is designed to help companies take the first steps towards more cybersecure business processes. However, ensuring information security is an ongoing process. Once the first steps have been taken, it is worth reviewing the [recommendations](#) for small institutions and companies in the Estonian Information Security Standard¹ – there, you will find the following activities to further improve information security in your company.

1.1 The responsibility lies with the head of the company

It should be mentioned that cybersecurity is not just a matter for the IT department, but also for management and executives. The clearer the business manager's understanding of the need to implement protective measures, the better they can direct their team and resources. Members of management play a key role in ensuring the information security of an organisation and their actions and decisions have a direct impact on the organisation's ability to protect its data and systems. Cybersecurity should not be a question of doing either everything or nothing. Here, too, it is possible to start small and move forward gradually – just as companies are already constantly reviewing and improving their business processes and working practices.

Here's what to do!

1. Make information security a strategic priority for your organisation and allocate financial, technical, and human resources to implement it.
2. Follow information security laws, regulations, and standards.
3. Map the organisation's responsibilities, liabilities, assets, and risks.
4. Define your organisation's level of risk tolerance and identify those responsible for information security.
5. Make sure to have an overview of the state of information security and possible incidents.
6. Carry out regular security training and contribute to raising staff awareness.
7. Create a working environment that values information security. Be a role model by following the best practices and policies on information security.

¹ <https://eits.ria.ee/et/abimaterjalid/veits>

2 Determine the company's security needs

Information security starts with a clear understanding of what we are protecting and why. Often, it is (small and medium-sized) companies that may not fully appreciate the importance of cybersecurity and the risks of inadequate information security.

Protection requirement is a set of security requirements that need to be met for an organisation's business processes to operate at a high level of quality. In order to assess the protection requirement, it is worth considering different loss scenarios, such as:

1. Which regulations and agreements set requirements or expectations for the organisation?
2. What is the potential harm to someone's life and health from the activities of the organisation?
3. What are the losses if the organisation's tasks are not completed and the quality of work is not as expected?
4. What are the consequences of damaging the organisation's reputation?
5. What are the financial consequences of data and system failures?

By considering various scenarios, the organisation can identify the weakest areas that need to be prioritised for protection. It also identifies risk tolerance, or risk criteria – situations where monitoring is sufficient and those where protective measures need to be implemented immediately.

In a digitalised society, it is essential for security to be a natural part of the company, which means that security risks are treated like any other business risk. Once the company has identified its protection needs, there is a clear purpose for implementing security measures. In addition, such mapping provides guidance for situations where a contract ends, the law changes, or there is a new subcontractor, and will lead to an immediate understanding of what needs to be changed in the company's security management.

3 Know what hardware and software you are using

In order to successfully protect the company's network, you first need to have an overview of what devices and software it uses. Therefore, making an inventory is the first and most important step in creating a secure system. If you do not know what devices or software may be on the network, you will not be able to detect unknown and unauthorised devices or software. It is precisely these devices or software that can be exploited by attackers to gain access to the office network. If you do not know that certain software is in use, you cannot organise its updating. There is also a risk of software being installed that could introduce malware (for example, illegal music/film downloading software). For each device that is on the office network, you should have the following information:

1. device ID or name;
2. manufacturer and model;
3. the serial number of the device;
4. IP address;
5. purpose of the device or the reason why it is in the network (computer, server, network device, etc.);
6. list of software installed on a device;

7. what business process it affects;
8. how the assets are linked.

3.1 Hardware inventory

First, you need to identify which devices are on the network. Even if it is a small network with only a few devices, the information must be documented. Failure to do so may cause these devices to remain unprotected. It is unprotected devices that attackers are looking for to gain access to the company's network. An overview of the devices on the network is also necessary when IT employees or service providers change, as they need to have information about the network and the devices on it.

If the company network comprises more than a couple of computers, it is recommended to use software that does the inventory automatically. Manual inventory can introduce errors, and it is very time consuming if you have many devices. The hardware register should also include any devices that are not currently in the network, but which may be connected to it or which could lead to data leaks if stolen.

3.2 Software inventory

Once you have an overview of the devices on your network, you need to find out what software is running on them. This is necessary to check that the software has been updated and that no unnecessary software has been installed on the devices. When taking inventory of software, it is also a good idea to use a tool that can automatically collect data. Among other things, the automatic software inventory helps to detect when new software has been added to a device. The software data collected should be linked to the device register so that all devices and associated software can be monitored in one place.

Ask an IT specialist

Both free and paid software is available for hardware and software inventory.

Paid software usually provides more functionality. Ask your IT employees or service provider for suitable software.

3.3 Consider implementing central device management

In order to better manage your devices and software, it is worth considering adopting a central management solution. Central management allows managing devices from one place and determining which software should be installed on devices, at the same time eliminating the need for several inventory software and management systems. Central management makes it possible to perform inventories as well as apply security requirements to devices. Some central management software makes it possible to remove data from devices over the internet, which is required if an employee loses a device or it is stolen.

Ask an IT specialist

A number of solutions are available for central management depending on which devices (computers, smart devices) are in use. They are usually paid software. Ask your IT department or service provider for solutions that are suitable for the company.

3.4 Establish rules for using personal devices in the working environment

Nowadays, it is increasingly common for employees to want to use personal devices for work. Smart devices (phones and tablets) are very common, but personal computers are also increasingly used. In addition, employees bring their own USB flash drives and external hard disks to work, allowing data to be quickly and easily moved from the internal network to external storage.

If employees are allowed to use personal devices, clear rules must be established, as these devices may also process company data. Where possible, the rules should be drawn up in cooperation with users and the IT department.

When creating rules for the use of personal devices, you must:

1. determine which security requirements are established for personal devices. For example, it is essential to require that devices are password-protected and have antivirus software installed.
2. Create a list of devices and operating systems that are not permitted in the company, such as devices with security vulnerabilities or devices that are no longer supported by the software manufacturer. Personal network devices (user's personal switches, routers, Wi-Fi devices, etc.) that may cause malfunctions in the company network should be prohibited;
3. if possible, keep a list of the devices that employees wish to use. It should include the employee's name, device name, software list, etc.;
4. establish clear instructions for the use of external storage media, such as USB drives and external hard disks;
5. if necessary, create a rule prohibiting the storage of work-related information on personal devices.

Users must read and agree to the rules and requirements and confirm it with their signature (otherwise, their personal device is not allowed to be used for work).

3.5 Assess the implications of using cloud services

Cloud services offer businesses great flexibility, cost savings, and better access to data. At the same time, they introduce new risks that must be consciously managed. The following principles will help you make informed decisions when choosing and using cloud services, while ensuring the security of your company's data.

3.5.1 Choose the right service provider

First, it is important to choose a service provider. Choosing a provider is a strategic decision that affects the security of your company's data – careful planning and an informed choice can

help to ensure that your business fully benefits from cloud services while minimising potential risks. Key considerations when choosing a cloud service provider:

1. Ensure that the service provider complies with relevant security standards and regulations.
2. It is important to know where the data is stored and how it is managed. This is important for data protection as well as regulatory compliance.
3. The reliability and availability of the service provider – information on past incidents and how the provider has resolved problems can be useful.
4. Good customer support is critical. It is worth making sure that the cloud platform provides timely and expert support.
5. What does the service cost and what are the terms of the agreement? It is important to ensure that the service does not involve any hidden fees or contractual obligations, especially regarding the return of data at the end of the service period.

Before making a decision, it is worth researching a number of service providers, comparing their offers, and reading customer feedback.

3.5.2 Use cloud services safely

Once you have found a suitable service provider, you should pay attention to the secure use of the cloud platform. Security settings – such as access control, network security, and logging – should be carefully reviewed during service setup. Many cloud providers offer built-in security features to help protect against cyber threats – such as filtering spam or malicious content. Regularly review these protections and, if necessary, enable additional safeguards on the management interface, making them mandatory for all users. A well-configured platform lays the foundation for success, but security requires ongoing attention, not just a one-time setup. Cloud systems need to be regularly maintained and updated to protect systems and prevent the exploitation of known vulnerabilities. In addition, logging and continuous monitoring of activities are essential to quickly identify any unusual behaviour. To achieve this, you must configure system logs and regularly monitor cloud activity to swiftly detect and respond to potential incidents.

Lastly, data backup must not be overlooked. The cloud does not eliminate the need for regular data backups – in fact, it makes them even more crucial. You should regularly back up your data and make sure it is stored securely. For certain services, the cloud provider may offer backups, but at least one backup should always be stored separately from the environment, either on a storage medium controlled by the organisation or in another cloud service. This ensures that data can be restored in the event of unexpected problems. You can read more about secure backup in chapter 7.3 ‘Ensure backup operation and verification’.

3.5.3 Ensure you know who has access to cloud services

Within the organisation, you must carefully define access to resources. Each employee should have only the access needed to complete their tasks.

With cloud services, a personal account is created for each user that is managed by the organisation. However, each account must be protected by a strong and unique password and multi-factor authentication. When using cloud services, ensure that the accounts of departing

employees are closed by their last working day to prevent access to the organisation's data. This can prevent situations where sensitive data is accessed by unauthorised persons. For more information on access rights and how to protect your accounts, see chapter 4.1 'Give access rights reasonably' and chapter 5 'Protect your employees'.

An administrator account has more privileges than a standard user account. Therefore, those responsible for managing cloud services should use a dedicated administrator account, distinct from their regular work account. When using cloud environments, it is essential that the organisation always retains administrative access to its own dedicated and isolated environment in the cloud. To ensure this, you should determine during setup how to restore administrative access with the specific cloud service provider if needed, and apply the necessary settings accordingly. For example, you may need to enter the administrator's contact details (such as an alternate email address) and securely store recovery codes outside the cloud environment, such as in a physical safe. Administrator accounts also need to be protected with a strong password and multi-factor authentication. Some cloud services allow you to restrict access to your organisation's user environment or management interface based on specific IP addresses or devices. It is also worth considering the use of conditional access policies, which allow you to control who can access services and under what conditions – such as location, device security level, time of day, or the application used. It allows for stronger, more flexible safeguards than static rules alone.

It is important to give clear instructions to employees on how to use cloud services and to make them aware of the risks associated with the platform. Informed and prepared employees can avoid many common security risks that may arise from carelessness or ignorance.

3.6 Use new technologies safely

Artificial intelligence (AI) and machine learning can help businesses grow, speed up processes, and reduce costs. However, it is also important to understand that new technologies come with risks.

Good to know!

RIA and Cybernetica AS investigated the risks of AI technology and ways to mitigate them in small and medium-sized enterprises. Read more here: <https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf>.

To use AI in a smart, responsible, and secure manner, a company must take deliberate steps to manage the associated risks.

1. Think carefully about why and how you are using AI

Before implementing AI, clearly define what you want to achieve – for example, what problem it solves, what data it will use, and how the system will be technically built. A clear system description is the foundation for understanding the risks involved.

2. Understand the full lifecycle

An AI system is not just about 'switching on the technology.' It has a beginning, development, active use, and ongoing maintenance. You need to map out the system's full lifecycle – from planning and data collection to deployment and continuous monitoring. It is important to maintain constant awareness and control because risks can arise at any stage. Determine who is responsible for each phase and what could potentially go wrong.

3. Ensure everything is legally compliant

If your AI system processes personal data (such as customer information), you must comply with data protection regulations such as the GDPR and possibly also meet additional industry-specific requirements. Make sure your activities are in line with the law and that you have obtained all necessary permissions and consents.

4. Consider who might be affected

Beyond technical and legal aspects, you should assess the broader impact. AI can affect customers, employees, communities, or even the environment. Think carefully about whether the system could create unfair outcomes, favour certain groups, or cause confusion and concern. Such risks might not be immediately visible but could have serious long-term consequences.

5. Assess risks and find solutions

After identifying potential risks, it is important to choose appropriate measures to mitigate them. Make a list of possible issues and evaluate how serious each one is. Then select suitable solutions – you might need stronger cybersecurity, clearer rules, or additional training for employees. A thoughtful approach to risk management will help to prevent problems and build user trust.

4 Protect your assets

Once you have a good overview of what devices and software are on your office network and used by your employees, you need to start protecting them.

As devices and services (website, business software, etc.) may be hosted by the service provider or already have some kind of software protection (firewall, antivirus), you may think that they are already protected. In reality, this is not enough to protect against threats. For effective protection of equipment and data, additional measures must be taken and protection must be actively addressed.

4.1 Give access rights reasonably

Attacks and viruses usually spread through users. The more rights the user has, the easier it is for the attacker or the virus to act.

Therefore, with every access it must be considered whether the access/rights (e.g. access to a shared folder, business software, or administrator's rights to a computer) are actually required for work. If it has been decided that they are really needed, the rights should be granted on the basis of the principle of least privilege, i.e. an employee should be given exactly as few rights as they need for their work and no more. Often companies take the path of least resistance and rights are granted to the whole catalogue, so an employee may have access to data to

which they should not have access. Even if the employee does nothing with this access, attackers can still exploit it.

Good practice!

Grant access rights through groups. This makes it easier to grant rights and provides you with a good overview. Then, when an employee leaves the company, it is easy to simply remove them from the relevant groups, rather than having to go through the catalogues one by one and find what they have access to.

Day-to-day work should be done with a standard user account, not an administrator account. There are a number of risks associated with administrator rights:

1. employees may install programs in their computer that may result in security vulnerabilities and malware;
2. the damage caused by malicious software is greater if employees have administrator rights;
3. the attackers can then more easily take control of a computer, etc.

However, if administrator rights are required, a separate administrator account with privileges should be created for that user, to be used only when necessary and not for day-to-day operations. This reduces the likelihood of a user inadvertently installing malware, and in the event of a leak of employee account details, the attacker will not immediately gain administrator rights. If it is an employee's personal computer, the rules in section 3.4 'Establish rules for using personal devices in the working environment' should be followed, but even then, a separate account for work-related matters is recommended.

Ask an IT specialist

Regularly ask your IT department or service provider for an overview of administrator accounts in use.

When the IT department or service provider grants access rights, they should also document when, where, and to whom access was given to maintain an up-to-date overview of access permissions. This information is also helpful when an employee leaves, as it indicates which accesses need to be closed. It is important to remember that access must be revoked and rights removed for individuals who have left the company.

4.2 Update software regularly

The use of software of all kinds is a normal part of work today. Vulnerabilities and other weaknesses are constantly being discovered in software that attackers can exploit to install malware, take control of a computer, and/or steal data. Regular software updates are therefore essential and one of the simplest activities to protect your company's assets.

If automatic software updates are available (e.g. for computers and smart device operating systems), they should be enabled. However, if the software does not contain that feature (for example, various programs or software for network devices), you will have to do it manually (by yourself or with the help of the IT department or service provider) or use a solution that

helps you do it automatically. For example, many of today's antivirus solutions offer functionality to help you conveniently and automatically update your programs.

If the software or hardware is no longer supported or updated by the manufacturer, it should be upgraded or replaced. For example, Microsoft will no longer support computers running Windows 10 starting in 2025. In this case, it is recommended to upgrade to the latest version of the Windows operating system or consider adopting an alternative operating system. Using outdated software can impact the device's security, compatibility, and support services, introducing various risks. For instance, new security vulnerabilities and flaws will remain unpatched, making the system more susceptible to cyber attacks. Even if no security issues have been discovered in the old software yet, it is only a matter of time before they are found and exploited. You may think about it this way: if there is a security vulnerability, there is an attacker who will be happy to exploit it. Good asset management helps to monitor, for example, the installation of updates or the need to install them.

4.3 Organise the protection of your company's computer network and its users

The boundary between the public Internet and the office network is called the perimeter. The less suspicious traffic there is entering the office network, the lower the risk to employees and devices on the network. The perimeter is protected by a firewall, which acts as a mediator or gateway between the public and office network, filtering out dangerous traffic. Firewalls with more features can detect and also prevent attacks against the office network. Such firewalls are also able to limit which pages employees are permitted or prohibited to access. For example, it is possible to block known dangerous pages or other suspicious pages that may be infected with viruses. You can also check which applications the employees use to access the Internet (for example, you can disable downloading films and music from the web).

As many viruses and attacks are delivered via email, it is essential to have antivirus and anti-spam protection on the email server. This software filters out suspicious messages (such as spam, phishing, viruses, etc.) to prevent them from reaching employees. Most email servers include some level of spam filtering. Spam protection can also be provided as an external service in the cloud or via hosted solutions (outside the office network), or as a separate server within the office network. Advanced spam protection software includes a number of features that make the life of employees easier – spam quarantine reports, email release options, sender blocking, and more.

As attackers are constantly finding new tactics, some malware still occasionally reaches users. It is therefore important that all devices are equipped with antivirus software to protect against it. When it comes to antivirus software, it is also important to ensure that it is the latest version, that it is up to date, and that all the functionalities are turned on, because otherwise the protection is not effective.

4.4 Prevent access to data in lost or stolen devices

There will inevitably be times when employees lose their devices (smartphones, tablets, laptops, etc.) or they are stolen. As the devices may contain confidential company data or other information that cannot be disclosed to third parties, you should plan ahead for what to do in that situation.

One feature that helps is the central management described in chapter 3.3 'Consider implementing central device management', which allows you to remotely lock, locate, or erase all data from a device in case of loss. Smart devices, such as phones and tablets, are also equipped with free apps that allow you to perform the same activities and they should be used.

Encryption can also help to prevent access to data. If a computer or external hard drive is stolen or lost, no one can read the data on it without the correct password or key. Encryption makes the data unreadable, which is especially important if it contains sensitive information (e.g. financial data, personal information, or trade secrets). Modern computers already have tools to encrypt data (such as BitLocker or FileVault). There are also other encryption software options that can provide additional security. It is important to remember that encryption works well only if you use a strong password and keep it in a secure place.

4.5 Ensure the physical protection of data and devices

In addition to software protection measures, you must also pay attention to the physical protection of devices. All devices containing important data must be protected from access by unauthorised persons. For example, a firewall does not help if a stranger can wander freely to the office, walk to the server room, and thus access the equipment directly.

Servers, network devices, and other important devices containing data must be stored in a separate device cabinet or a dedicated server room. The door to the device cabinet or server room must be locked and the key kept in a safe place. You should also maintain a log of server room visitors – including who accessed it, when, and for what purpose – to ensure traceability and accountability.

Ask an IT specialist

If the server is located in a hosted environment, ensure the service provider has information about who has physical access to the server and who has used it.

For the server to run smoothly, it needs to be sufficiently cooled (air-conditioned server room) and connected to a UPS to protect it from power outages. Otherwise, the server may stop running on hot summer days or data may be corrupted if the power fails.

If there are unused network sockets in the office, you should not be able to access the network from these sockets (have your IT department or service provider disable the access). Otherwise, you could have a situation where a random person connects their computer to the network and can access all the devices in the office. The next step would be to configure the computers and servers to be on separate networks, i.e. if someone can access the computer network, they cannot immediately access the servers as well. Separate Wi-Fi networks should be set up for employees and guests to prevent strangers accessing the company's internal network.

It is equally important to teach employees to lock their computers when leaving their workstation, avoid leaving devices unattended in public places, and prevent unauthorised access.

5 Protect your employees

In order to protect data and users, it is important that any access to systems requires a password or other means of authentication. The password must be sufficiently complex to be difficult to guess. If the system is not password-protected or the password used is easily guessable, both malware and attackers will have much easier access to the system. This may result in data leakage or the destruction or modification of important data.

5.1 Create a secure password policy

Authentication is the process by which the system verifies that the person accessing the system is who they say they are. Usually, a password or certificate is used for authentication.

To keep your office network secure, you need to set rules on password complexity and length. You should change your password immediately if there is any suspicion of password leakage or an incident takes place. All accounts – including work, personal, and social media accounts – should use different passwords. A good password is strong (at least 15 characters, including special symbols) and unique. Instead of a typical password, it is recommended to use a passphrase. The phrase may consist of four or five words, which form a sentence (for example: 1Horse.Is.By.The.Wat3r) – it is longer, but easier for users to remember than a password made up of random characters. The password should use uppercase and lowercase letters and a symbol (full stop, comma, exclamation mark, etc.) between words. The password should be easy to remember, but not too easy to guess.

If the system configuration allows, restrictions should be applied automatically, as users tend to choose the path of least resistance. If it is not possible to set it up automatically, the regular password changes must be done manually and the users must be constantly reminded to do so. Smaller companies usually do not have a separate password policy, but it is essential to create passwords in accordance with good security practice.

Ask an IT specialist

Ask the IT department or service provider if the current password policy is in line with good practice. If necessary, a password policy must be created and implemented.

5.2 Use multi-factor authentication

Due to the growing popularity of cloud services, companies have increasingly more services that are publicly available around the world. If the service is available to the public, it is easier to attack. If a commercial service (such as Office 365, Gmail, Dropbox, etc.) supports it, multi-factor authentication should be enabled. This means that, in addition to the password, some other authentication method is required, such as entering a code, confirming on a phone, using an ID card, a cryptographic token, or a hardware solution like a YubiKey.

If multi-factor authentication is implemented, attackers cannot access the system even if the password is leaked, as they lack another authentication component.

5.3 Simplify the use of passwords

As most systems require the use of passwords, employees may have many usernames and passwords. In this case, users will start writing them down on paper, possibly using the same password in several places, or choosing passwords that are too simple. One solution to help users is to use password management software that enables them to manage their passwords securely. There are various pieces of software available for this purpose, some of which are free.

If there are many devices, it is worthwhile to deploy a central user management solution. For example, the Active Directory (AD) domain is available in Microsoft Windows for this purpose. The AD domain is a service that enables integrated authentication in a Windows environment. This allows users to log in with the same username and password to all devices in the domain. For example: before the domain was introduced, users had separate passwords for their computer, email service, and shared folder; with the domain, the user can access everything with a single password. The AD domain requires a Windows server. There are other similar solutions that do not require a server, such as Azure AD, which requires Office 365 software licences. Some business software can also be linked to, for example, AD domain or Azure AD. Centralised user management makes it easier to revoke access when a user leaves, as it can be done from a single location.

6 Learn to recognise attacks

A system is only as secure as its weakest link. Unfortunately, the weakest link is often the users themselves. Therefore, cybercriminals often try to access the system through users by sending them emails with viruses or phishing letters to try to steal passwords, bank details, or money. There are also websites on the Internet that try to scam users out of data and money, or contain viruses. Employees must therefore be taught how to recognise these attacks and how to respond to them. Informing and educating employees is also one of the most important steps for protecting the company.

6.1 Raise employee awareness

In recent years, cybercriminals have evolved considerably and it is increasingly difficult to tell whether an email sent or a website visited is fraudulent.

Employees should be made aware of the most common attacks, how to recognise them, and how to respond to them. IT employees or the service provider can help you to provide this information and guidance.

If any of the emails you receive looks suspicious, it is always worth contacting your IT department or service provider and asking them to inspect the email. Even if the email turns out to be genuine, it is better to be safe than sorry.

Employees should be trained to recognise fraudulent and phishing emails and dangerous websites in the following way.

1. Check the sender's email address – although it sometimes appears genuine, the sender's address is usually slightly changed. For example, instead of '@eesti.ee', the sender might use something like '@eetsi.ee'. Sometimes, replying to the email, even if

the address appears genuine, can reveal that the recipient is someone other than the sender.

2. In the case of websites, check their address. As with email addresses, the website address may have been changed, for example, to '.ea' instead of '.ee' at the end of the address, or numbers added to replace letters in the address, for example, 'eest1.ee' instead of 'eesti.ee'.
3. Any emails and websites promising money, travel, free things of value, etc. are very likely to be scams.
4. If the email appears to be from the company's board or accountant, you should check that the style of the letter is as usual, especially if it requests a transfer of funds. Usually, fraudulent letters are suspiciously short and threatening in tone ('Pay now, it must be paid within 24 hours!', etc.).

6.2 Train your employees

In addition to improving the overall cybersecurity level of the company, cybersecurity awareness training should be organised for employees. The training must cover security issues in general: behaviour on social media, use of public cloud services, secure use of Wi-Fi, etc.

A training plan could include:

1. learning about the company's IT security rules, security requirements, and risks;
2. an analysis of the risks of various devices and services (portable devices, social media, public cloud services, etc.);
3. behaviour in the event of security incidents (who to notify, what to do, etc.);
4. recognising possible threats and the most common attacks, assessing the consequences of such attacks;
5. an analysis of recent security incidents that have become public along with a description of the causes and possible prevention methods. One way to train employees is to join the cyber test offered by RIA. This is an e-learning platform designed to raise and maintain the cybersecurity awareness of an organisation's or company's employees. We update the content of the cyber test every year. You can find more information about the cyber test on [the website](#) of RIA.²

6.3 Regularly check your employees' knowledge

In order to check whether the general guidance and training of employees is producing results, their knowledge needs to be checked regularly. It helps them to remember what they have learned and keep it fresh in their mind. Knowledge can be tested, for example, by means of surveys that can be offered by various companies providing cybersecurity services or training – they are also the best placed to update these tests. This way, the company will also receive information on whether employees should be retrained on some topics.

It is also a good idea to organise small drills to check employees' behaviour – for example, by sending them a fake phishing letter. The results of these tests will show what else you need to tell your users or whether additional training is required. Inform people about the results of the

² <https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/kubertest>

incident analysis and involve them in the development of the rules. This way, they are motivated to follow the rules themselves. The knowledge of staff can also be checked using the cyber test outlined in section 6.2 'Train your employees'.

7 Prepare for incidents and learn to recover

Inevitably, there will be situations where data (files, emails, databases, etc.) are deleted or corrupted. This may happen because an employee accidentally deletes a file or overwrites a file with wrong data. In addition, cyber attacks and theft of devices or accidents (fire, flood) can occur that destroy or corrupt data. It is crucial for a company to have a plan in place for handling incidents and to ensure that all important data is backed up and stored securely.

7.1 Be prepared with a clear plan of action in the event of an incident

Inform the RIA Incident Handling Department CERT-EE (cert@cert.ee) about the occurrence of a cybersecurity incident. For additional consultation and incident analysis, the organisation must be prepared to share details of the incident and have a designated contact person authorised to communicate with CERT-EE.

In the event of an incident, start by documenting the situation:

1. save local and log server logs;
2. preserve configuration (e.g. firewall rules);
3. create disk images of affected systems;
4. save at least the last backup before the incident, and if possible, all backups of systems involved in the incident up to that point.

Once the situation is identified, define the scope of the incident, which includes mapping all affected systems. Compromised or potentially compromised systems should be isolated immediately.

During the recovery of IT services, it is important to avoid losing relevant evidence (logs) during the system restoration process. As a result of the root cause analysis of the incident, actions should be planned to prevent similar situations in the future.

In the event of a cyber incident, it is crucial to inform your clients or partners who are affected by the incident. In certain cases, such as a personal data breach, companies are obligated to notify the Data Protection Inspectorate. Additionally, during the resolution of the incident, consider whether a report should be submitted to the police.

7.2 Create a recovery plan

It is important to have a recovery plan to ensure business continuity. While it may seem that you know how to restore a system in the event of a failure, Murphy's Law suggests that you will need to recover it during the company's busiest working hours, when the most knowledgeable specialist in that particular system is not available. In this case, a recovery plan can help you to restore the system quickly and correctly in the most critical situation.

The recovery plan must set out in detail all the information necessary for restoring the systems that are important for the company:

1. the people responsible for restoring the system, as well as their contact details;

2. description of hardware and software – all devices, tools, data, and software versions required for restoration with their exact location;
3. step-by-step process guide – what to do and in what order;
4. settings of the system to be restored;
5. users required for restoration (service accounts, administrator password, etc.).

In the event of a cyber incident, documents stored on the server may not be accessible, which is why it is a good idea to keep a printed copy of the recovery plan in a pre-agreed location.

7.3 Have a clear overview of what is happening in your systems

In addition to protecting IT systems, an organisation must have a good understanding of what is happening within them. This helps to detect potential attacks more quickly and understand how an attacker gained access.

To achieve this, logging must be properly configured and the recorded log data must be monitored. It is important that all necessary information is included in the logs – for example, network traffic, security devices, domain controllers, servers (including administrative actions), workstations, and applications. Logs should be retained for at least 1 year, preferably up to 3 years. This is necessary to determine, in the event of a security incident, when the suspicious activity began and which systems were affected – because an attacker may be present in the systems long before anything noticeable happens.

Logs should be stored on a separate server and backed up, so they are preserved even if the main system is compromised. It is also advisable to implement a monitoring solution that tracks system performance and security incidents, and sends automated alerts if needed, to enable a quick response to problems.

7.4 Ensure backup operation and verification

When planning a backup, the first step is to determine what data is important to the business and needs to be backed up. Everything you need – emails, business software databases, shared directories, and files – should be backed up and the data on users' computers should be also taken into account. Among other things, it is also necessary to back up the data required for system recovery, such as the configuration files of servers or network devices and other technical information.

Second, it is also important to determine how far back the backup data should go. Important data, such as shared folders used on a daily basis or business software, may need to be backed up daily and retained for a month, for example (meaning that it is possible to restore data that is a month old). Data that does not change frequently (such as an image bank or archive) can be backed up once a month, with only a single copy kept.

Ask an IT specialist

Arrange the backup (type of data, frequency, number of copies) with the IT department or service provider.

An external backup should also be made to protect the backup copy in the event of an accident (fire, flood) or theft. That backup can be stored in the cloud, in another office, or, for example, hosted by a service provider. In addition, it is worth keeping one backup on a storage medium that is isolated from the network. When using a cloud service or external provider, keep in mind that your data will be hosted by a third party. Carefully consider whether it is appropriate to store backups of confidential data or trade secrets in such environments.

It is also important to ensure that backups are successful, as data cannot be recovered from a failed or corrupt copy. To do this, set up email notifications to confirm that backups are running, and regularly review the backup logs to ensure that the backups are completing successfully. It is a good idea to check periodically that all the necessary data is still backed up (for example, a folder may have been moved to another location and not configured for backup) and, if necessary, change the backup settings. In addition, it is important to keep documentation on backups: what kind of data is backed up, where it is backed up to, how many backups are kept, and which software is used for the process.

7.5 Perform recovery testing

Regular recovery testing is very important. It involves restoring an important part of the system to a separate location from the current system (so that the working environment is not affected) and checking that everything is working after the restoration. Recovery testing is important because even if it seems that the backup copies have been successfully made, there may be errors during system restoration that cannot be foreseen. For example, a backup may be invalid, data may be missing, or additional settings may be required to restore the system. Any anomalies or special settings detected should be documented in the recovery plan. Recovery testing must be performed for all important systems and the backup for testing should be selected randomly.

Ask an IT specialist

Ask the IT department or service provider if there is a recovery plan for the recovery of the company's systems and whether they have performed recovery testing. If necessary, a recovery plan must be created and recovery testing arranged.

8 Protect your brand

The company's brand is associated with public websites, social network accounts, and email addresses. As they are publicly visible, there is a risk that attackers will want to use them to damage the company's reputation, to make money, or for some other reason. It is therefore important that they are protected.

8.1 Acknowledge potential risks

Public services (websites, email) are exposed to threats that can disrupt business operations and damage their reputation.

Examples of risks that public websites may face include:

1. Attackers can make a company's website inaccessible. This paralyses, for example, an e-commerce company and also disrupts the work of many other businesses because customers may not get the information they need from the website.
2. Attackers can gain access to website management and steal, for example, company customer data, which may result in reputational damage and GDPR fines.
3. Attacks can make the content of the website inappropriate (e.g. offensive), which may once again interfere with the work of the company and damage its reputation.
4. Attackers can install software on a website that infects visitors with malware. This will lead to a situation where the company's customers will start avoiding the website, even after it is fixed.

Good to know!

The GDPR is the European General Data Protection Regulation, which sets out guidelines for the processing of personal data in the European Union. Violating the GDPR can result in heavy fines: €20,000,000 or 4% of the previous financial year's turnover, whichever is greater. Fines may apply in the event of an incident if, for example, the company has ignored the implementation of technical and procedural security measures. Read more here: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_et.

When social network accounts are taken over by attackers, it can result in reputational damage (inappropriate posts, insulting customers, etc.) as well as financial damage for the company if the accounts are linked to payments (for example, credit card information is included to buy Facebook ads, which attackers can access). In addition to the company's own social network accounts, the accounts of the company's management and key employees should also be protected.

If the company's email service lacks proper protection, attackers can exploit business email addresses to scam employees or partners or to send spam. Emails sent from an unprotected domain may also get caught in the spam filter of an email server and not reach the recipient. This can lead to both reputational damage and financial losses.

8.2 Protect the company against threats

The first step in protecting the company against threats is to be aware that they exist. There are a number of actions that companies can take to protect themselves against threats.

8.2.1 Select tools to detect security vulnerabilities

Attacks on public services usually exploit vulnerabilities in the software of the service (e.g. a website or an email server), weak security settings, overly simple or leaked passwords, etc. There are tools to automatically detect security vulnerabilities. Such tools scan public services and generate comprehensive reports of detected security vulnerabilities. Once they are detected, the IT department or service provider should remove them. You will then need to run a new scan and check whether the security flaws previously detected have been resolved.

They need to be scanned on a regular basis (e.g. once a month) to consistently detect and eliminate new vulnerabilities.

Ask an IT specialist

There are various solutions for detecting security vulnerabilities. Ask your IT department or service provider for the appropriate software.

8.2.2 Protect your public services

To protect public services, the security vulnerabilities identified must be addressed. It is also important that the software of the websites or the email server is up to date (see section 4.2 'Update software regularly'). Both the service server and the service's own software must be updated.

To protect your domain, ensure that the contact details listed in the domain registry for domain management are accurate and up to date. CERT-EE monitors the .ee domain space and sends notifications to the owners of pages with critical security flaws or compromised pages. Accurate data ensures that notifications reach their destination on time.

Ask an IT specialist

If the server is hosted and managed by a service provider, confirm with them that the server software is updated regularly and ask when the last update was performed.

To protect the email service, the IT department or service provider must make the following configurations:

1. To protect the data exchange between mail servers, you must enable TLS support for the SMTP protocol, use POP3s and IMAPS protocols, and disable support for unencrypted POP3 and IMAP protocols on the server side. It is important to use only trusted certificates issued to the correct FQDN (fully qualified domain name) for email server services, and the certificate should also be allowed to be used for email protection;
2. In order to prevent attackers from freely using company email addresses, an SPF protocol (Sender Policy Framework) should be created in the DNS, stating which email servers can send messages under the company's email domain. When using mass email senders (such as Smaily, MailChimp, etc.), they should not be added to the SPF record; instead, DKIM should be used. Otherwise, it may happen that all users of the same service can send emails on behalf of someone else.
3. In order to authenticate the company's email server, it is also possible to configure DKIM (DomainKeys Identified Mail). DKIM signs the email messages leaving the server, while other email servers check that the signature is valid.
4. DMARC (Domain-based Message Authentication, Reporting and Conformance) distributes a policy to email servers via DNS that says what should be checked in an email from that domain and how the email server should handle it. DMARC uses SPF and DKIM to verify compliance with its policies. With DMARC, it is possible to receive

a report on whether someone has attempted to send emails from locations that are not authorised.

Good tips and advice on protecting your email service can also be found on RIA's [blog](#).³

8.2.3 Protect your social network accounts

Social network accounts, such as X, LinkedIn, Facebook, Instagram, etc., are often attacked. The company's management and key employee accounts are also at risk and must be protected in the same way.

To protect your company's social media accounts, you should take the following steps, which are not complicated at all, but will significantly increase security:

1. Create a corporate social media policy. Among other things, the rules should cover:
 - which social media channels (platforms, accounts, and pages) the organisation uses and their intended purposes;
 - which employees have access to the account, including their roles and permissions;
 - the procedures for maintaining back-up access to accounts;
 - the process for transferring access when roles change or employees leave;
 - expectations for employee conduct on social media.
2. Use strong passwords and update them whenever an employee with access to company accounts leaves the organisation.
3. Turn on multi-factor authentication.
4. Regularly check existing social media accounts. Always remove access for staff who no longer need it.
5. Check the account settings. From time to time, platforms may update their privacy settings or the existing settings may change.
6. If accounts are not actively used, they should still be protected and monitored in the same way as actively used accounts to detect possible takeovers.
7. If you use an external service provider to manage your platforms, ensure that your organisation retains full ownership of all accounts and content through a clear agreement.

Ask an IT specialist

If your company is active on social media networks, it is worth considering using a software solution designed to protect social media accounts. This allows, for example, the automatic removal of suspicious content, prevention of unauthorised content from being published, detection of other accounts created using the company's brand, and so on. Ask your IT department or service provider about these solutions.

³ <https://www.ria.ee/blogi/taga-oma-organisatsioon-e-kirjavahetuse-usaldusvaarsus-ja-turvalisus>

9 Pay attention to the supply chain

Imagine that the same IT service software is being used simultaneously by a law firm, a retail chain, and a construction company. Instead of attacking each organisation individually, it may be easier for a malicious actor to breach the software they all use – gaining access to each of their systems through a single point of entry. This is known as a supply chain attack.

Such attacks can disrupt system operations, corrupt data, and lead to leaks of sensitive information. They often result in both financial losses and reputational damage.

If you use software or hardware from another company (a third party), you must be aware that this also introduces supply chain security risks.

To reduce these risks, it is advisable to:

1. verify whether the service provider has undergone security audits, and whether these audits cover the topics relevant to your organisation;
2. sign a contract that specifies, for example, log management, network monitoring, access rights distribution, and network segmentation;
3. define specific security requirements for services and products and include them in the contract;
4. agree on designated contact persons and communication procedures in case of issues;
5. establish clear actions to be taken in the event of service disruptions or other security incidents;
6. regularly request system monitoring reports from the service provider.

Please remember!

Check whether the cybersecurity requirements outlined in the contract are being followed and determine how the service provider handles incidents, vulnerabilities, security patches, and compliance with security requirements.

Special attention should be given to supply chain risk management. This includes documenting service providers and identifying the risks associated with using third-party software or hardware. To reduce risks, it is worth consulting the risk management guidelines of the Estonian Information Security Standard (E-ITS), as well as its broader implementation.⁴

⁴ <https://eits.ria.ee/>