101 on cyber hygiene – from the perspective of mothers, fathers and employers

Cyber hygiene isn't that different from regular hygiene: find some suitable products that clean and protect, use and change them regularly and stick to a routine.

Keep your devices and accounts secure

All smart devices, from your computer to your phone, must be equipped with passwords and anti-virus software. The easiest way to protect your data is to set passwords for all your devices, regardless whether they are used to surf online, or they are controlled and configurated through the internet. Anti-virus software is also mandatory. Passwords and other user IDs must be kept in a way that they wouldn't be accessible to third parties. You should change passwords regularly. If you suspect that someone has become aware of them or that someone has an unauthorized access to you device or account, change all related IDs immediately.

It's never a good idea to login to your e-mail or social media accounts in a public or an unknown device (i.e. phones or tablets displayed in IT-stores). Firstly, people tend to stick to their habits even in unknown devices, which means that there is a strong possibility that you might forget to log out afterwards or you might download content that you didn't mean to share with third parties. Secondly, an unknown device might save the passwords of your accounts without your knowledge and signing out won't help, because you've already unwillingly given access to your accounts to third parties.

What to keep in mind as an employer

Employers and employees should think about whether and how the data will be secured in case an employee won't show up to work one day. If only one employee has access to certain systems and something happens to them, then the employer may suffer significant damage in the form of unfinished work and lost data. This can be avoided if the employer maps out all work processes, concludes confidentiality agreements with the employees and unequivocally and clearly instructs the employees in using devices and data. The employer should consider that if the employee breaches the current law or legislation that will soon enter into force, the employer will be accountable for the employee's violation and possible damages. It's not even always about misusing the personal data, but also about keeping the employer's trade secrets confidential and their reputation spotless.

The younger generation is extremely comfortable when using different social media and messaging apps, as well as other platforms created for personal information exchange, and they forget that some information is not allowed to be shared nor stored on those platforms. Especially if the employer hasn't stated that those platforms are official channels of communication. All private conversations that an employee has had on Facebook messenger or their phone will permanently be stored there, and the employer has no means to delete them or make sure that the information and files will be deleted.

In addition, you should keep in mind that the employer has no overview about the contractual relationships that the employee has with their service providers. Often the users have no control over whether, in what amount and when these platforms store their information. Organizations, public authorities and non-profit organizations have the obligation to process all personal data securely and to give an overview about the stored data to the subject if necessary. That also applies to e-mails and phone numbers.

What do minors do online? What can a parent post about their child?

A parent or a guardian is a person who is responsible for the child's safety. If a minor has uploaded inappropriate content or sent sexual pictures or videos about themselves, it's reasonable to wonder where their parents were at that time. As the adult, a parent has the obligation to explain to the minor about the risks and dangers related to using smart devices. The parent should firstly make sure that they themselves understand all the possibilities of different devices and then decide whether their child should come in contact with those dangers at all.

Posting content about minors (even by their parents or guardians) is also considered to be processing of personal data and the priority is to protect the child's interests. You should never forget that no posts can ever be erased permanently. The audience in social media grows with every „Like" and share of a picture. Anyone can download pictures once they have been displayed on their screens. A picture of an infant or a toddler that you shared with your close relatives can become available to perverts in an instant. Even if the parent never receives any information about the fact that a sick person has repeatedly abused a picture of the little person, a child's everyday life can be affected if their peers find that a post is worth making fun of. The most sensible and lawful decision is to not post pictures of your children on social media.

Third persons do not have the authority to create accounts for children without their parent's or guardian's consent. Education facilities also have the obligation to ask their subjects for consent about forwarding their data to third parties. Forwarding children's personal data to third parties is probably in violation with the current law. Therefore, it's absolutely unacceptable for schools to create accounts for kids that have possibilities that the school isn't even aware of. Accounts that were created to be used in lessons can then be used by the students to post content that might endanger them. IT education in general education schools must comply with the current law and must in its essence prevent danger.

Make smart choices regarding your devices, social media, accounts, e-mails and ID-cards

People don't acknowledge the fact that others' computers, tablets, phones, e-mails and messaging platforms are not meant to be read or used by third parties. Violation of message secrecy is i.e. a situation, where the other person's phone messages are read (without permission) etc. Saying that there shouldn't be any secrets in close relationships is not a valid argument. Devices must be protected with passwords. No one has the right to ask you for any user IDs for your accounts, devices etc. Don't let anyone snoop around in you accounts or devices.

Situations where a family member has illegally used an ID-card that has been easily accessible, along with its passwords and other documents that have been stored in the same drawer, are quite common. Main accounts of ID-card fraud have been related to transferring money from the owner's bank account, signing small loan contracts and contracts of suretyship or gambling online. An ID-card is an equally important document to a passport. However, unlike passports, ID-cards can be used to conclude transactions that the owner of the card hasn't intended to make. Those kinds of transactions are void, but it is up to the owner of the card to prove that it wasn't them who made the transaction, because it's impossible for a bank employee to know if the digitally signed document is signed by anyone else but the person shown in the digital container. The victim's passiveness brought on by embarrassment, also doesn't help to void the transaction, since it means that the victim isn't willing to turn to the police and the other party of the transaction immediately after discovering the violation. The longer you wait to report this information, the harder it will be for the police to carry out the investigation.

Keep in mind that crimes expire and that civil transactions will stay in effect if the victim doesn't dispute them in time.

KATRIN SARAP
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
KATRIN.SARAP@NJORDLAW.EE

LIISI JÜRGEN
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE