Let's talk about cybersecurity

Let's get started

Coffee breaks discussions

Online meeting ideas

Interreg Baltic Sea Region
Co-funded by the European Union
RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

Lets´t talk about cybersecurity!

Conversations over the coffee are most enjoyable when they are interactive. This is also the case when it comes to cybersecurity.
It is quite typical that someone talks about cybersecurity and others listen. But that does not have to be the case. Coffee breaks in the working places are a great opportunity to take everybody into account: ask questions and listen.

It's also easier to notice if something is not understood, and to explain in more depth: *“What in the earth I´m going to do with the VPN?”* The discussion will help you to understand what people really wants to know about cybersecurity.

Often, cybersecurity issues are far from the minds of ordinary people. People don't really know how things relate to their lives. Why should they need to understand how multi-factor authentication works or how to protect their email account - *“I don't have anything important there!”*

It is important to show how cybersecurity is relate to the world of even the most ordinary person. What could happen to him if he can no longer access his email, why anyone can become a cybercrime victim, what things are of value to a hacker...

Coffee breaks in the working place are important for the well-being of employees. And remember, when working remotely, chatting with colleagues is just as important.

This guide was also built through joint discussions and interaction. See the link tips on the last page!

Interreg Baltic Sea Region
Co-funded by the European Union
RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

What is cybersecurity?

Liza

Cybersecurity refers to the actions needed to protect network and information systems and network users from cyber threats. Cybersecurity covers both the software and the operations that keep devices and information secure.

Data security, information security and data protection are also used in everyday language, how do they differ from cybersecurity?

Mirjam

Cybersecurity is the process of ensuring the security of information, information systems and devices in a networked environment. Cybersecurity aims to prevent damage caused by malicious software. Data security or information security covers the broader issue of securing information. It also includes the physical storage of information outside the digital environment and the prevention of misinformation.

The data protection and privacy laws relate to the proper collection and use of personal data. You have the right to know what information is collected and stored about you by online services and you have the right to request its deletion.

I don't have to worry about data security because I have nothing to hide!

Think again. People usually lock the door of their house when they leave home because they don't want thieves to get in. Nowadays all kind of information is stored in the digital world, and it's a good idea to keep the doors leading to it locked.

I think I should make a list of all the digital doors and windows I have.

Laura

Leena

Do you have an email to log in to online services? What would happen if someone took over your social media account? Don't forget that you also have online banking credentials. Is your credit card number public information? Your health information and your prescription are also information you don't want others to see.

Uh, I can't remember many different passwords! I hate our IT-Team when they require me to change my password.

Hackers need passwords and usernames to take over accounts. Login credentials are stolen in data leaks all the time.

Hackers use passwords and usernames to try to hijack other online accounts as well. Hackers can simply try different passwords. Computer programs can go through billions of passwords per second.

Nick

Lilly

Criminals can obtain login information by phishing. Hackers can ask unsuspecting victims for their login details by email, SMS, scam sites or even by phone.

What is a password management application?

Lin

The Password Manager application helps you to store your passwords for different online services. You only need to remember the master password. Other passwords are stored behind the master password.
The app can recommend a strong password when you register for a new service.
There are free and paid apps, locally installed or running in the cloud.

Jean

Are password managers safe?

Password managers are meant to protect your most sensitive digital information, such as login credentials and payment card details. It prohibits you to reuse your passwords. A trusted password manager enables you to create long and unique, and unguessable combinations.

What is a good password policy in an organization?

Complexity requirements	Minimum length	Regular password changes	Multi-Factor Authentication (MFA)	Education and training
Require passwords to be complex.	Set a minimum password length to ensure passwords are sufficiently long and harder to crack.	Encourage or mandate regular password changes helps maintain security and reduce the risk of compromised passwords.	Implement MFA wherever possible, especially for accessing sensitive systems or data.	Provide ongoing education and training to employees about the importance of password security and best practices.
This complexity makes passwords harder to guess or crack through brute-force attacks.	Longer passwords are generally more secure, for example minimum 12 characters.	For instance, requiring employees to update their passwords every three to six months	MFA adds an extra layer of security by requiring users to provide multiple forms of verification.	Make sure the employees know how to create strong passwords.
Always include a mix of uppercase and lowercase letters, numbers, and special characters.	A strong password might include a phrase to enhance security and to be easier to remember.	Don´t ever reuse the passwords or pass phrases.	MFA can for example be a combination of a password and a temporary code sent to your phone.	Understand the risks of password reuse.

That phishing simulation our IT department organized was an eye-opener. It's astonishing how easy it is to fall for a scam

Now that I've learned to recognize phishing emails, it feels like I encounter them constantly!

I almost clicked on that link until I noticed the URL was wrong. Can't be too careful with these things.

Jack

I was almost fooled by that email, but luckily, I realized in time that it wasn't real.

It's concerning how phishing attempts come from so many different channels now. We really have to be vigilant in emails, social media, and texts.

Carmen

How to recognize an online scammer?

Unexpected messages	Too good to be true offers	Urgency and pressure	Request for personal information or money	Poor communication and presentation
Scammers often initiate contact unexpectedly.	If an offer seems too good to be true, it probably is.	Scammers often create a sense of urgency to pressure victims into making hasty decisions.	Be wary of requests for personal information or money from unknown sources.	Suspicious websites or emails might have unusual URLs, mismatched logos, or other signs of amateurism.
They can use email, social media messages, or phone calls.	Scammers often lure victims with promises of large sums of money, incredible deals, or opportunities that seem unrealistic.	They might claim that an offer is only available for a limited time or threaten consequences if you don't act immediately.	Be cautions especially if they claim it's necessary to claim a prize, resolve an issue, or access a service.	Scammers may use poor grammar, spelling mistakes, or low-quality graphics in their communications
Be cautious if you receive a message from someone you don't know or weren't expecting to hear from,	Always verify the legitimacy of such offers through reputable sources before proceeding.	Take a step back and carefully evaluate any situation that requires a rushed response	Legitimate organizations typically don't ask for sensitive information or payments without proper verification.	With the help of AI some scammers have become more sophisticated in their presentation.

My dear colleague, may I point out that the screen should be locked whenever you leave your desk.

Uh, I just went to the bathroom, and besides, there's nothing interesting open on my computer.

Locking the screen is a good habit, sometimes you might go away for a bit longer and if you don't lock the screen anyone can read your email.

Layla

I think it would be a good idea to make a poster that remains us about safety behavior in cybersecurity.

Peter

I guess we can find cybersecurity check-lists on the DistanceLab-project website!

Tool usage and security				
File encryption	Cloud security measures	USB device management	Secure file sharing	Regular security audits
Utilize file encryption tools to protect sensitive data stored on local devices, USB drives, or cloud storage.	Implement robust security measures for cloud storage solutions, such as multi-factor authentication (MFA).	Establish policies and procedures for USB device usage within the organization to mitigate the risk of data leakage or malware infection.	Use secure methods for file sharing, both internally and externally,	Conduct regular security audits.
Encryption scrambles the data in such a way that only authorized users with the decryption key can access it.	This helps safeguard data stored in the cloud from unauthorized access, data breaches, or cyberattacks.	This may include restricting the use of USB devices to authorized personnel.	Encrypted file-sharing platforms and secure file transfer protocols (such as SFTP or HTTPS) ensure that files remain protected during transit.	Identify vulnerabilities in tools, systems, or processes related to file management and security.
Encryption improves security, especially if the device is lost or stolen.	“The principle of least privilege” means granting access to data only to those who truly need it.	Scanning devices for malware before use, and encrypting data stored on USB drives, increases safety.	Prevent unauthorized access or interception of sensitive information.	This proactive approach allows organizations to address any weaknesses.

It's crucial to remember to maintain security while working remotely. I've heard that remote connections can be easier targets for accessing company data.

I've started using two-factor authentication even when working on my home network. It's better to be safe, especially when the network's protection might not be as strong as in the office.

Julia

I was just thinking, how do we ensure that all data remains secure when so many people are working remotely from different locations?
VPN is probably the solution, right?

Gregor

I've installed the company-provided security software on my home computer too, to avoid accidentally sharing confidential information.

I had to go through that security training again recently, as it emphasized the risks specific to remote work. One can never be too careful.

Why are updates important?

Security updates	Bug fixes	Compatibility	Features and improvements	Compliance and support
Updates often include security patches that fix vulnerabilities discovered in the software.	Updates also frequently include bug fixes that address software issues or disruptions.	Compatibility issues may arise when using older versions with newer operating systems or hardware configurations.	Updates sometimes introduce new features that improve functionality, usability, or performance.	In many cases, using outdated software may lead to compliance issues with industry regulations or standards.
By keeping your software up to date, you ensure that these vulnerabilities are patched promptly.	Running outdated software may lead to performance problems, crashes, or other usability issues.	Newer versions of software often introduce compatibility improvements with other programs or devices.	By staying current with updates, you can take advantage of these improvements to streamline workflows.	Additionally, vendors typically provide support and assistance only for the latest versions of their software.
Reduce the risk of cyberattacks and data breaches.	An outdated software can disrupt productivity and user experience.	By staying updated, you ensure that your software can work seamlessly with the latest operating systems, hardware, and third-party integrations.	Updates may improve productivity, or access new capabilities.	By staying updated, you ensure that your organization remains compliant and receives timely support when needed.

I feel powerless, I no longer dare to use the internet!

Many worries can be minimized by taking a little time to plan ahead. For example, you can prevent malware and viruses by using antivirus software and keeping your software up to date.

Anne

Routines and regular checks create security. Get into the habit of updating your computer whenever it asks for it (don't press the "later" button but restart your computer as soon as possible).

Daniel

Your Internet traffic goes through many servers before connecting to the site you are using. In a "man in the middle" attack, someone intercepts your traffic along the route and sees what you do on the Internet, including your password and username. Attacks are often carried out over public and unsecured Wi-Fi networks. You can protect yourself with reliable VPN software.

Backups are also part of your security. Make sure your work is safe.

I am not motivated to do my job because there are more threats than opportunities.

The current world situation is exhausting. As technology advances, the pace of working life is accelerating. At the same time, cyber threats are increasing. It is becoming increasingly difficult to judge which programs are safe. Going through privacy policies is frustrating.

Ali

It's worth discussing the issue. Especially for those working remotely, it is worth regularly discussing current concerns. Loneliness, busyness, and stress can make you vulnerable to cyber-attacks.

Emma

How do I know what information is right and wrong?

Follow news from trusted sources. Don't share information on social media that you can't verify.

Remote work and cybersecurity				
Secure Remote Access	Device Security	Data Protection	Awareness Training	Regular Security Assessments
Ensure that remote access to company systems and data is secure.	Implement policies to secure remote devices used for work, such as laptops, tablets, and smartphones.	Establish guidelines for handling and storing sensitive data while working remotely.	Provide remote employees with cybersecurity awareness training to educate them about common threats.	Conduct regular security assessments and audits to evaluate the effectiveness of remote work security measures
Use virtual private networks (VPNs).	This includes installing antivirus software, enabling firewalls, implementing device encryption,	Encourage the use of secure file storage and sharing solutions, such as encrypted cloud storage or company-approved file-sharing platforms, to prevent data breaches.	To fall in phishing scams, social engineering attacks may increase while working alone.	Identify potential vulnerabilities. This includes assessing remote access controls, device security configurations, and compliance with security policies and procedures.
Use multi-factor authentication (MFA).	Remember regularly updates.	Do not discuss confidential matters out loud on the phone in public transportation or cafes.	Empowering employees to recognize and respond to security threats can help prevent security incidents.	This proactive approach allows organizations to address any weaknesses.

Learn more about cybersecurity:

DistanceLab:
https://interreg-baltic.eu/project-posts/distance-lab/remote-business-strategy-pilots-how-to-participate/

Other EU-financed project wort to take a look:

Cyber citizen
https://cyber-citizen.eu/en/

Down load “Cyber city tycoon” -game
https://play.google.com/store/apps/details?id=com.aalto.cybercitizen&pli=1

Cyber-resilient Kymenlaakso
https://www.xamk.fi/en/project/cyber-resilient-kymenlaakso/

ISSUES - Information Security and digital Services for sUstainablE designS
https://www.cybernorth.se/

Women4Cyber
https://women4cyber.eu/

Pictures in this guide:
Adobe Stock, Canva

Interreg
Baltic Sea Region

Co-funded by
the European Union

RESILIENT ECONOMIES AND COMMUNITIES

Distance LAB

https://interreg-baltic.eu/project/distancelab/