Interreg
Baltic Sea Region

Co-funded by
the European Union

RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

LET´S TALK ABOUT CYBERSECURITY

Interreg
Baltic Sea Region

Co-funded by
the European Union

RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

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

Let’s 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 want 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!

WHAT IS CYBERSECURITY?

Cybersecurity covers both **the software and the operations that keep devices and information secure**.

It refers to the actions needed to **protect**

- **network**
- **information systems**
- **network users**

from cyber threats.

Data security, information security and data protection are also used in everyday language.

How do they differ from cybersecurity?

Cybersecurity ensures

- the security of information,
- the security of information systems and devices in a networked environment.

It 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.

DATA PROTECTION & 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.

LAURA

LEENA

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

Good idea!
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 prescriptions are also information you don't want others to see.

WHICH ONLINE SERVICES HAVE INFORMATION ABOUT YOU?

____

____

____

____

____

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

UH, I CAN'T EVEN REMEMBER **MANY DIFFERENT PASSWORDS!**

Hackers use passwords and usernames to try to hijack other online accounts as well!

They can simply try different passwords. Computer programs can go through billions of passwords per second.

NICK

LILLY

I hate our IT-Team: they always require me to change my password.

IT-Team is your friend!
Ask them for a trusted password management app!

It helps you to store your passwords for different online services. You only need to remember the master password!

WRITE HERE EXAMPLES OF
LOUSY PASSWORDS
NOBODY SHOULD EVER USE!

____

____

What is a good password policy in an organization?

Complexity requirements

- Complex passwords make it harder to guess or crack through brute-force attacks.
- Always include a mix of *UPPERCASE* and *lowercase letters*, *numb3rs*, and *speci@l characters*.

Minimum length

- Set a minimum password length to ensure passwords are harder to crack.
- Longer passwords are generally more secure, for example minimum 12 characters.
- A strong password might include a phrase to enhance security and to be easier to remember.

“IUSEDtoRUNwithMYDOGat0900!”

Regular password changes

- Encouraged or mandatory regular password changes help maintain security and reduce the risk of compromised passwords, e.g. requiring employees to update their passwords every 3-6 months.
- Don´t ever reuse the passwords or pass phrases.

Multi-Factor Authentication (MFA)

- can e.g. be a combination of a password and a temporary code sent to your phone.
- implement wherever possible, especially for accessing sensitive systems or data.
- adds an extra layer of security by requiring users to provide multiple forms of verification.

Provide ongoing education and training to employees about the importance of password security and best practices.

CRIMINALS CAN OBTAIN LOGIN INFORMATION BY PHISHING.

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

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

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

And I got a mail about a delivery of a product I never ordered!

It's concerning how phishing attempts come from so many different channels now. Hackers can ask unsuspecting victims for their login details by email, SMS, scam sites or even by phone.

ASK YOUR COLLEAGUES ABOUT
WHAT KINDS OF PHISHING ATTEMPTS THEY HAVE NOTICED:

How to recognize an online scammer?

Unexpected messages

- Scammers may contact you unexpectedly via email, social media, or phone.
- Be cautious with messages from unknown or unexpected sources.

Too good to be true offers

- Offers promising large sums or unreal deals may be scams.
- Verify the legitimacy of such offers through reliable sources.

Urgency and pressure

- Scammers use urgency to rush victims into decisions.
- Be wary of limited-time claims or threats and evaluate situations calmly.

Request for personal information or money

- Avoid sharing personal info or money with unknown sources.
- Legitimate organizations verify before requesting sensitive information.

Poor communication and presentation

- Look for unusual URLs, mismatched logos, or poor grammar as scam signs.
- Some scammers use AI for more sophisticated presentations.

My dear colleague, may I point out that THE **SCREEN SHOULD BE LOCKED** WHENEVER YOU LEAVE YOUR DESK!

Oh! But 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

PETER

I would really need some reminders and a poster about safety behavior in cybersecurity...

We can find cybersecurity check-lists on the DistanceLab-project website!

REMEMBER CYBERHYGIENE!

Tool usage and security

File Sharing

- Use tools to encrypt data on devices, USB drives, and cloud storage.
- Encryption ensures only authorized users can access data.
- Encryption improves security, especially if the device is lost or stolen.
- Protect files from unauthorized access or interception during transit, encrypted file-sharing platforms ensure that files remain protected.

Data access

- Implement multi-factor authentication (MFA) to protect data from unauthorized access and breaches.
- Apply the principle of least privilege to limit data access to necessary personnel.

USB Device Management

- Establish policies and procedures for USB device usage within the organization to mitigate the risk of data leakage or malware infection.
- Scan for malware.

Regular Security Audits

- Conduct audits to identify vulnerabilities in file management and security processes.
- Address discovered weaknesses proactively to enhance security.

It's crucial to maintain security while **WORKING REMOTELY.** I've heard that remote connections can be easier targets for accessing company data.

True! I've started using two-factor authentication even when working on my home network. The protection might not be as strong as in the office.

How do we ensure that all data remains secure when people are working remotely from different locations? VPN, right?

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

Working remotely, I worry more! I feel alone with my concerns and I feel there are more threats than opportunities.

JULIA

GREGOR

It's worth discussing the issue! Working remotely loneliness, busyness, and stress decrease your wellbeing and may make you more vulnerable to cyber-attacks. There is also a chance to fall into social engineering: those attacks that try to appeal to your emotions!

INVEST ON WELLBEING AND MAKE SURE ALSO THE REMOTE WORKERS FEEL INCLUDED IN THE WORKING COMMUNITY. THIS WAY THEY ARE ALSO MORE COMMITTED TO THE COMPANY INSTRUCTIONS AND PRACTICES.

Remote work and cybersecurity

Secure Remote Access

- Ensure that remote access to company systems and data is secure.
- Use virtual private networks (VPNs).
- Use multi-factor authentication (MFA).

Device Security

- Implement policies to secure remote devices such as laptops, tablets, and smartphones.
- Install antivirus software, enable firewalls, implement device encryption.
- Remember regular updates.

Data Protection

- Establish guidelines for handling and storing sensitive data while working remotely.
- 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.
- Do not discuss confidential matters out loud on the phone in public transportation or cafes.

Awareness Training

- Provide remote employees with cybersecurity awareness training about common threats.
- Empowering employees to recognize and respond to security threats can help prevent security incidents.

Regular Security Assessments

- Assessments and audits evaluate the effectiveness of remote work security measures.
- Identify potential vulnerabilities: includes assessing remote access controls, device security configurations, and compliance with security policies and procedures.
- Proactive approach allows organizations to address any weaknesses.

1. WHO CAN ENTER YOUR WORKSPACE? ____________________
2. DO OTHER PEOPLE HEAR YOUR CALLS? □ YES □ NO!
3. DO YOU USE PUBLIC NETWORKS? □ YES □ NO!
4. WHO DO YOU TURN TO WITH YOUR
   CYBER SECURITY QUESTIONS? ____________________

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.

Routines and regular checks create security. I try to get into the habit of updating my computer whenever it asks for it.

Good! No more pressing that “Later” button!

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

"MAN IN THE MIDDLE" ATTACK

YOUR INTERNET TRAFFIC GOES THROUGH MANY SERVERS BEFORE CONNECTING TO THE SITE YOU ARE USING.

SOMEONE MIGHT INTERCEPT YOUR TRAFFIC ALONG THE ROUTE AND SEES WHAT YOU DO ON THE INTERNET, INCLUDING YOUR PASSWORD.

BEWARE OF PUBLIC AND UNSECURED WI-FI NETWORKS AND PROTECT YOURSELF WITH RELIABLE VPN SOFTWARE.

Why are updates important?

Security updates

- They often include security patches that fix vulnerabilities discovered in the software.
- Reduce the risk of cyberattacks and data breaches.

Bug fixes

- Updates also frequently include bug fixes that address software issues or disruptions.
- Outdated software may lead to performance problems, crashes, or other usability issues.
- An outdated software can disrupt productivity and user experience.

Compatibility

- Compatibility issues may arise when using older versions with newer operating systems or hardware configurations.
- Newer versions of software often introduce compatibility improvements with other programs or devices.
- By staying updated, you ensure that your software can work seamlessly with the latest operating systems, hardware, and third-party integrations.

Features and improvements

- Updates sometimes introduce new features that improve functionality, usability, or performance.
- You can take advantage of these improvements to streamline workflows.
- Updates may improve productivity, or access new capabilities.

Compliance and support

- Using outdated software may lead to compliance issues with industry regulations or standards.
- Vendors typically provide support and assistance only for the latest versions of their software.

LEARN MORE ABOUT CYBERSECURITY:

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

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

- Download “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/

Pictures in this guide:
Adobe Stock, Canva, DistanceLab team