



Reduce stress & Boost your Cybersecurity Wellbeing

12.12.2024 Cyberakuten

Laura Palovuori

interreg-baltic.eu/project/distancelab



Digital safety culture

- Cybersecurity covers devices, software, and the operations that keep devices and information secure.
- Digital safety culture introduces the personal aspects of behavior, social interactions and daily actions



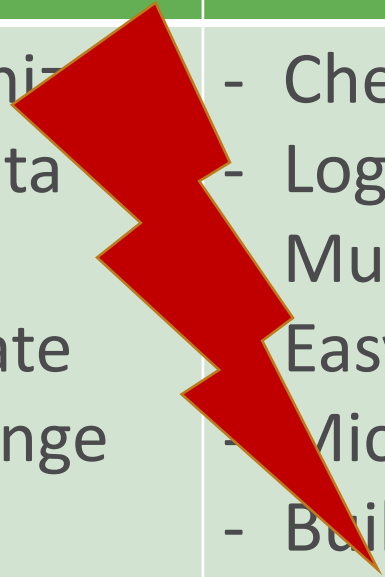
Does cyber security affect your wellbeing?

Digital Safety Practices

- Only click links you recognize
- Consider what personal data you share
- Keep your devices up to date
- Use strong passwords, change them often

Daily actions of most people

- Checking emails in a hurry
- Logging to open WIFIs
- Multitasking
- Easy to remember passwords
- Micro breaks online
- Build relationships



As an employer responsibilities pile up You might even feel alone

- Handling sensitive business data
- Handling customer data
- Fulfilling the expectations on staff regarding cyber security
- Safe working environment

“We all work remotely. In the office we could talk about things. Now our shared space is in the cloud, we talk by typing, we leave a lot more documentation digitally than we would if we were all in the office face to face”.

Stress...

Attention to sources of stress

→ What was left unfinished

→ Whether anything was annoying

→ Did I succeed today

Stress

→ Constant pressure

→ No chance to recover

→ Regulation of emotional reactions

What helps you to recover?

→ During the day

→ After the works

→ Remember to breathe



Quick tips for improved digital safety culture

Plan your work...

Knowledge
Learning new things
Adequate tools

A reasonable amount of work
Clear calendar
One thing at a time
Avoid interruptions
Mute beeps
Quiet working environment

Refresh your memory
To-do-lists
Set aside time in your calendar
for planning
Quiet planning days
Feeling that you have time to do
things as well as you would like
to

“I change passwords a couple of times a year. Once it happened that an outsider visited my Facebook, and I've become more careful since then”.

Routines help to reduce stress

Make data security a routine

Check for software and device updates every Monday morning

Make password change days in your organisation

Discuss and educate

Practice together

Identify critical information

What at least needs to be protected?

Make a list of the digital services your company uses

Which ones are free?

What are the payment dates for purchased services?

Which of these support your data security? For example, cloud backups and the updates of your website...

**“Cybersecurity certainly spoils the fun,
but maybe it would be easier if it became
routine”.**

Don't stay alone

Do one thing at a time!

Think, what kind of message needs an immediate response. ????????

Communicate with
your staff

Do you know
who to call if
you get
scammed?

Don't work when
you're tired or
stressed.

Remember to take
breaks, even if
you're working
distance.

What can an employer do to ensure good wellbeing at work AND improve cyber security practises?

- ✓ Learn about your staff's preferences, motivation and attitudes
- ✓ Connect online and offline – provide low threshold forums
- ✓ Leading cyber security with fear might shut off your staff
 - ✓ Provide up-to-date devices and software

“It would be fun if someone else took responsibility for cybersecurity. At the same time, I think I have to have control over everything myself. That's why I'm self-employed, so I can do everything myself”.

Passwords, updates, MFA, VPN

- Use different passwords for different services.
- Keep your devices and software updated.
- Implement multi-factor authentication MFA.
- Don't use open networks, rather share your phone's network with your laptop. If you absolutely must connect your laptop to an open network, turn on a VPN to protect your connection.
- Change the default password for your home network.

Keep your eyes open

- Your bank, tax authority or police will never ask for your bank details by email or SMS.
- If you receive a bill that seems strange, call the sender to confirm the situation.
- Don't believe everything you find on social media.
- Don't share false information. Check the accuracy of news on the websites of international news agencies.



DistanceLAB in short

Project duration: 1.1.2023-31.12.2025

Participating countries: Finland, Sweden, Norway, Poland, Lithuania, Latvia

Financed by: Interreg Baltic Sea Region

Lead partner: Centria University of Applied Sciences, Finland



LET'S TALK ABOUT CYBERSECURITY



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.



PETER



LAYLA

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

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

REMEMBER
CYBERHYGIENE!



CZUJĘ SIĘ BEZSILNY,
NIE MAM JUŻ
ODWAGI
KORZYSTAĆ Z
INTERNETU!

Rutyny i regularne kontrole zapewniają bezpieczeństwo. Postaram się wyrobić w sobie nawyk aktualizowania komputera za każdym razem, gdy widzę przypomnienie.

Wiele zmartwień można zminimalizować, poświęcając trochę czasu na planowanie z wyprzedzeniem. Na przykład, można zapobiegać złośliwemu oprogramowaniu i wirusom, korzystając z oprogramowania antywirusowego i aktualizowania.

Dobrze! Koniec z wciskaniem przycisku „Przypomnij później”.

ANNE



DANIEL



PRACIWNIK I INTERNET

TWÓJ RUCH INTERNETOWY PRZECHODZI PRZEZ WIELE SERWERÓW, ZANIM POŁĄCZY SIĘ Z WITRYNĄ, Z KTÓREJ KORZYSTASZ.

KTOŚ MOŻE PRZECHWYCIĆ TWÓJ RUCH NA TRASIE I ZOBACZYĆ, CO ROBISZ W INTERNECIE, W TYM TWOJE HASŁO.

UWAŻAJ NA PUBLICZNE I NIEZABEZPIECZONE SIECI WI-FI I CHROŃ SIĘ ZA POMOCĄ NIEZAWODNEGO OPROGRAMOWANIA VPN.

Kopie zapasowe (backup) są również częścią bezpieczeństwa. Upewnij się, że Twoja praca jest bezpieczna.

Dlaczego aktualizacje są tak ważne?

Aktualizacje zabezpieczeń

- Często zawierają poprawki zabezpieczeń, które usuwają luki wykryte w oprogramowaniu.
- Zmniejszają ryzyko cyberataków i naruszeń danych.

Poprawki błędów

- Aktualizacje często zawierają również poprawki błędów, które rozwiązują problemy z oprogramowaniem lub zakłócenia.
- Nieaktualne oprogramowanie może prowadzić do problemów z wydajnością, awarii lub innych problemów z użytecznością.
- Przeszarżowane oprogramowanie może zakłócać produktywność i komfort użytkownika.

Kompatybilność

- Problemy z kompatybilnością mogą pojawić się podczas korzystania ze starszych wersji z nowszymi systemami operacyjnymi lub konfiguracjami sprzętowymi.
- Nowsze wersje oprogramowania często wprowadzają ulepszenia kompatybilności z innymi programami lub urządzeniami.
- Pozostając na bieżąco, zapewniasz, że twoje oprogramowanie może płynnie współpracować z najnowszymi systemami operacyjnymi, sprzętem i integracjami innych firm.

Funkcje i ulepszenia

- Aktualizacje czasami wprowadzają nowe funkcje, które poprawiają funkcjonalność, użyteczność lub wydajność.
- Możesz skorzystać z tych ulepszeń, aby usprawnić pracę.
- Aktualizacje mogą poprawić produktywność lub uzyskać dostęp do nowych możliwości.

Zgodność i wsparcie

- Korzystanie z przestarzałego oprogramowania może prowadzić do problemów ze zgodnością z przepisami lub standardami branżowymi.
- Dostawcy zazwyczaj zapewniają wsparcie i pomoc tylko dla najnowszych wersji swojego oprogramowania.

Recruiting and working remotely?

Cybersecurity measures for remote work recruitment

- Audit for remoteworkers
- Employee Declaration at the End of Employment
- Your Day at Distance -app



Cybersecurity measures for remote work recruitment



Co-funded by
the European Union

REGIONS AND COMMUNITIES

LAB

In cooperation with Centria University of Applied Sciences and South-Eastern Finland University of Applied Sciences.



Euroopan unionin
osarahoittama

The DistanceLAB project is financed by Interreg Baltic Sea Region.

The Future of cyber security in Kymenlaakso project is financed by the Kymenlaakso just transition fund (JTF).

KYMEN
LAAKSON
LIITTO



centria
ammattikorkeakoulu

Cyber- and data security audit form for distance work

Remote workstation	Your answer	Your own notes about your situation	How you can reduce your risk.
Can you lock the door to your remote working space?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Sometimes		Lock your workspace whenever possible. Discuss with your employer whether they would be interested in paying for an electric lock, for example.
Does your remote working space have a lockable locker or cupboard?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Sometimes		Lock your equipment and documents in a cupboard whenever you leave the premises (during lunch, at the end of the working day). Discuss with your employer whether they are interested in paying for a lockable cupboard in the room.
Are there other people (non-work colleagues) in your workspace when you are working?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Sometimes		Can you turn the screen to not to be visible to others? Get a privacy film for the screen if this is not possible.
Do other people hear what you say during your working day, even if they are in a different room?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Sometimes		Close the door. Use headphones. Lower your voice. If it is a confidential matter, go to a place where no one can hear the conversation or ask outsiders to leave.

Once the person has been recruited

- Ensure that people working remotely receive regular training.
- The desire to learn is an important quality in all work, and in remote work it is really important to be curious and want to get to know things.
- It is important that everyone stays up to date on cybersecurity issues (not just the IT department).



After employment

- The employee promises on a signed form that the employer's company information or customer information is not available on the home computer, in the cloud or on paper.
- Ensure that the former employee does not have user credentials, permissions or access to the organization's systems.



Project's objective is to:

increase the resilience of the businesses in Baltic Sea Region by providing tools, skills and capabilities of thriving in remote business environments.



Get in touch with DistanceLAB



You'll find us @distancelab in Facebook and LinkedIn!

You can get to know the project on website:

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

LinkedIn: <https://www.linkedin.com/company/distancelab/>

and Facebook: <https://www.facebook.com/distancelab>

Remember to like and follow!



Interreg
Baltic Sea Region



Co-funded by
the European Union



RESILIENT ECONOMIES AND COMMUNITIES

Distance LAB



Thank you!

laura.palovuori@centria.fi

Illustrations by Adobe Firefly





DistanceLAB tools

