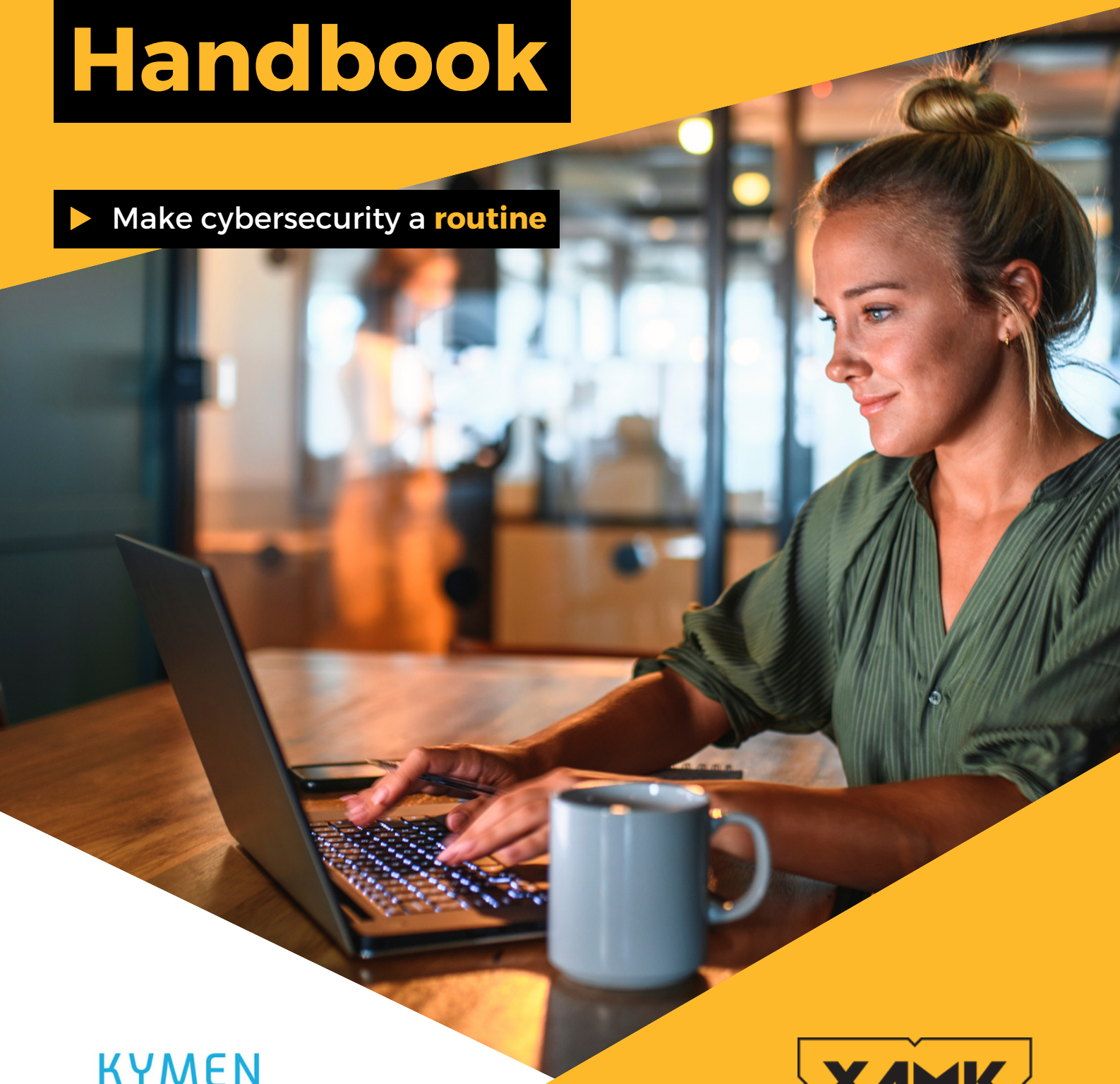
Cyber Hygiene

Handbook

▶ Make cybersecurity a **routine**



KYMEN LAAKSON LIITTO

XAMK
Kaakkois-Suomen ammattikorkeakoulu

This handbook

is a guide produced by the Satamalogistiikan kyberhygienia project. It can help **You** live and work safely in data networks, both now and in the future.

TABLE OF CONTENTS

What is cybersecurity?

Cybersecurity refers to the actions that companies, organisations and individual people take in order to protect digital materials, such as systems, devices and user accounts.

Basically, the idea is the same as when protecting **physical belongings**.

We want to protect our home and belongings from outsiders, so we lock the doors. Likewise, we lock a computer terminal because we want to protect the computer and the data in it from outsiders.

Cybersecurity is everybody's business!

Cybersecurity concerns **all of us**,

since each of us has a role to play in safeguarding digital materials. It's easy to see that criminals attack technical systems, since technical systems have technical weaknesses.

Likewise, it's understandable that we humans are also attacked. Humans have human weaknesses that criminals can exploit.

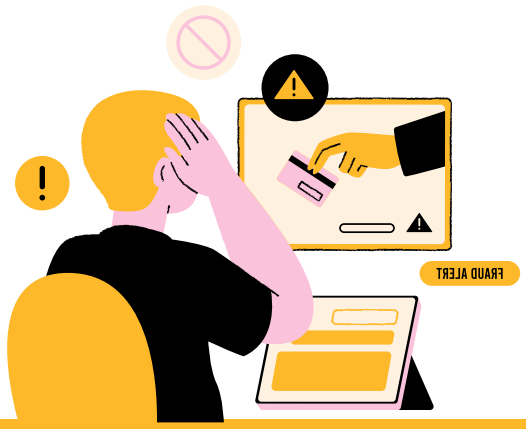
As humans, we are vulnerable to cyber attacks that exploit human weaknesses.

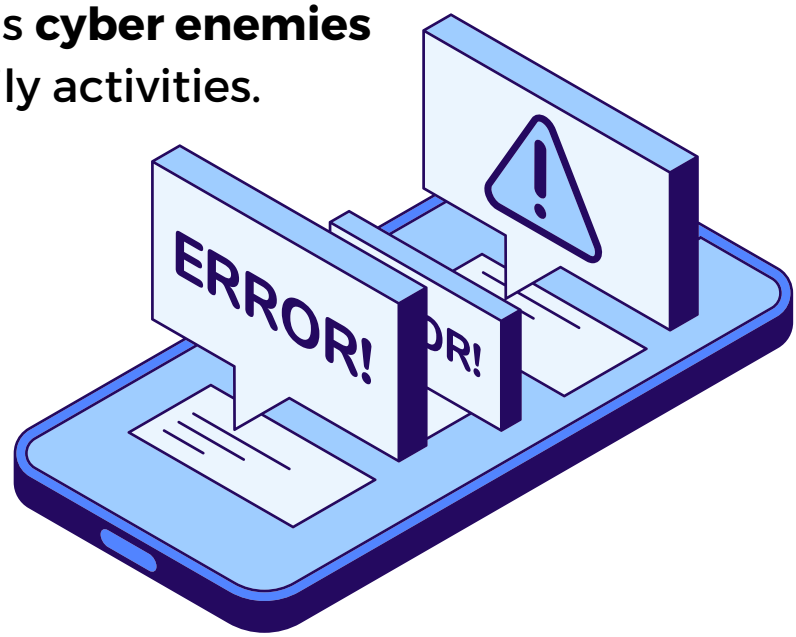
Cybersecurity is a **skill** which you can and must develop.

It's just like using the door to your home: the door protects the contents relatively well if you keep it locked. Careless actions, such as keeping the key under the doormat or leaving the door open, provides criminals with an easy way inside.

Know your cyber enemy

Cyber threats are threats to cybersecurity. You can also think of them as **cyber enemies** that we encounter in our daily activities.

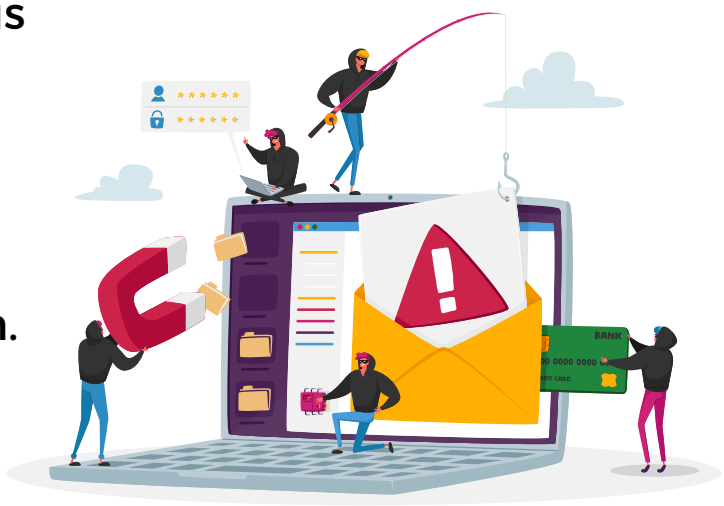




The most common cyber enemies are **phishers** and **social engineers**.

Phishers

Phishers are the most widely known and discussed type of cyber enemy. Phishers try to trick us into opening a malicious e-mail link, attachment, etc.



Their goal is to steal our important information.

The term phishing comes from the fact that these cyber enemies try to fish for our information by luring us with different baits.

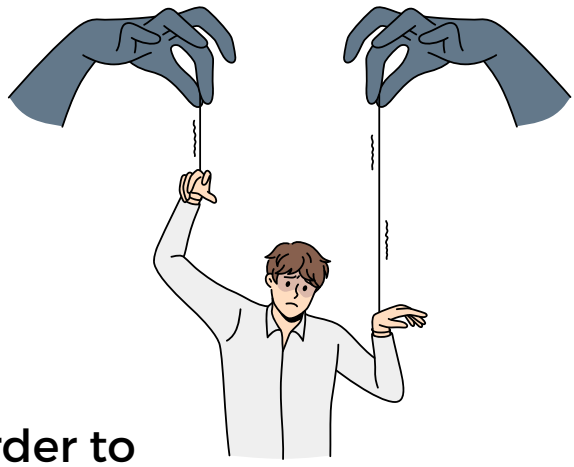
Phishers have various baits

Some baits are **identical** for everyone; a phisher casts huge numbers of them into the internet and hopes that someone takes the bait. One example of these are spam messages.

Some baits are **tailored** for individual targets; such baits are more likely to make the victim give their information. One example of these are fake invoices.

Social engineers

Social engineers try to manipulate us into acting in a way that is favourable to them.
They exploit our human weaknesses, such as our desire to help others.



Social engineers are cunning.
They know which strings to pull in order to successfully manipulate their victims.

Social engineers have a diverse toolbox. Here are some of their tools:

Scam messages

The social engineer sends a message and pretends to be someone else, such as a company's CEO.

Impersonation

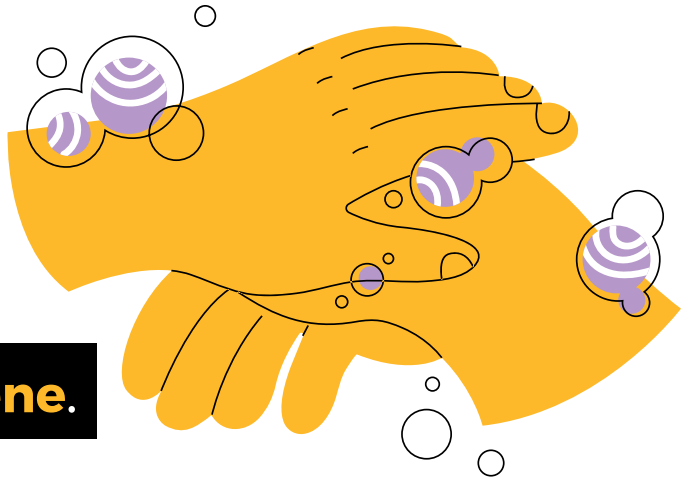
The social engineer impersonates a repairman and tries to enter a company's premises without being stopped.

Harmful USB sticks

The social engineer leaves harmful USB sticks in visible places and hopes that someone will connect one to their computer.

Personal cyber hygiene

Cyber enemies are indeed clever and know how to fool people. Despite this, we don't have to be afraid of them. In a way, the situation resembles the physical world and our daily encounters with different pathogens. Pathogens attack our immune defences, and we protect ourselves against them with good hygiene.



Cyber hygiene works in much the same way as regular hygiene.

Cyber hygiene means developing and maintaining cybersecurity, i.e., promoting cybersecurity for ourselves and our environment through regular routines.

The routines of cyber hygiene are meant to be as important and as easy as the routines of regular hygiene. For example, washing our hands is a simple routine that quickly becomes normal.

Good cyber hygiene helps us keep our **everyday lives safe**.

HOW TO TURN CYBER HYGIENE INTO A ROUTINE

Cyber hygiene can become a routine if you pay attention to the following: 1) **attitude** and 2) **getting started**.

1 Cyber hygiene is achieved by making safe operations a part of your daily routines. This requires that you pay attention to it. Cybersecurity is not a top priority for everyone, but we must all be aware of its importance and take the **necessary steps** to stay safe from cyber enemies.

2 Another key issue is getting started on cyber hygiene. Start with small actions that help you make cyber hygiene **a routine**. For example, you can decide to lock your computer whenever you leave it unattended. Start with this small routine and gradually add others, such as working correctly with passwords.

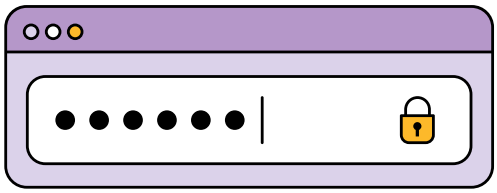
Cyber hygiene is that simple. But it does require the right attitude. Start with small things and keep cyber hygiene a part of your daily routines!

Small actions have a big impact

Here are five ways to improve and maintain good cyber hygiene.

1

Work correctly with passwords



Don’t use the same password for different services and never reveal your password to others. Remember to use long passwords (16 characters minimum). One good type of passwords are passphrases, such as **Acatwenttotherooftoseethegorilla**.

2

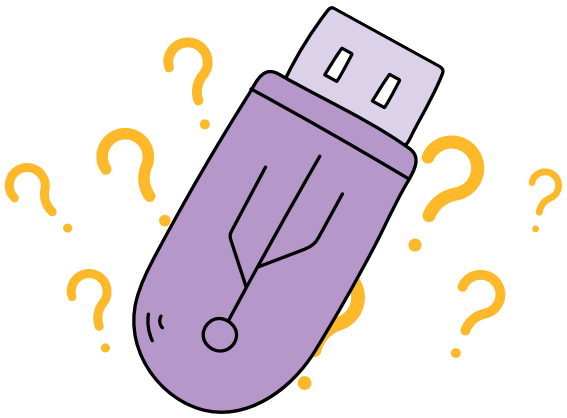
Think before you click

Don’t click on suspicious links or open dubious attachments. Links can lead to malicious websites and attachments can install malware on your device.

3

Lock your device

Lock your computer **every time** you move away from it. Even getting a cup of coffee can take long enough for a cyber enemy to do something serious to your computer.



4

Avoid unfamiliar devices

A mysterious USB stick on the ground may seem interesting, but it can also infect your device with malware. Avoid unfamiliar devices and **never connect them to your computer**.

5

Question what you see and hear

Don't believe everything you see or hear. Scam websites can look real, voices can be fake, and attacks can seemingly come from someone you know. These days, you must be critical and question the information you encounter.

In other words, cyber hygiene is a way of thinking.

These five actions are a good addition to your daily activities – but this isn't a complete list.

The most important thing in cyber hygiene is not to take specific actions, but rather to be aware of your own activities and **consider whether they are safe**.

Cybersecurity and occupational safety

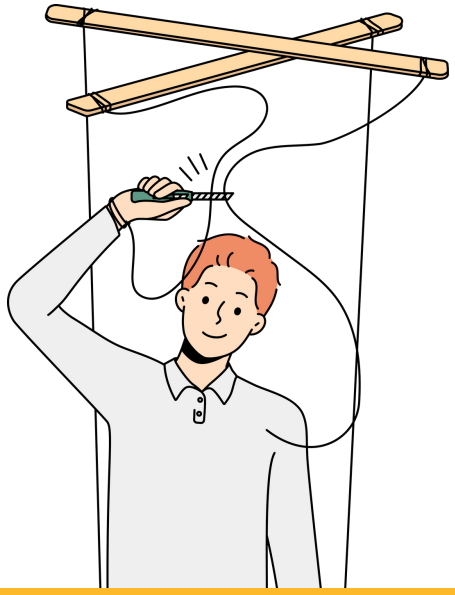
Cybersecurity is a part of **occupational safety**.

Both of these apply to everyone working in a company.

A company's management is, of course, responsible for the implementation of cybersecurity and occupational safety.

However, everyone in the company should remember that careless actions can give cyber criminals **easier access** to the company's systems.

If this happens, cyber enemies might even cause serious effects in the physical world. In other words, occupational safety may also be affected.



Don't be an easy target for cyber enemies!

Careless actions make life easier for criminals, and we don't want that. By taking safe actions, you maintain your own safety and the safety of your entire work community.

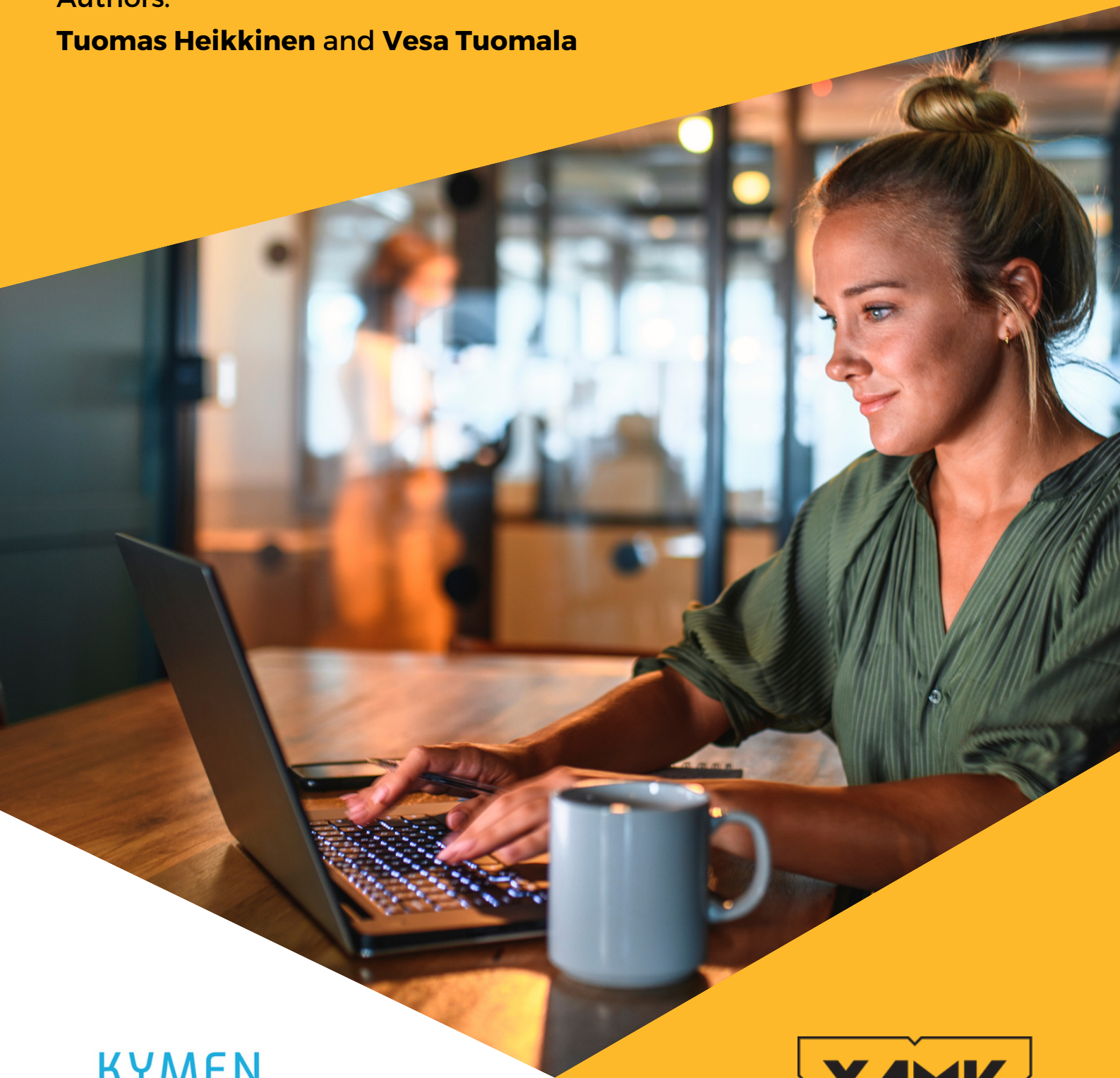
So don't be an easy target for cyber enemies.
Maintain good cyber hygiene.

Make life difficult for criminals

by acting in a cybersecure fashion!

Satamalogistiikan kyberhygienia (Cyber Hygiene for Port Logistics, project-number 13300047) is a project funded by the Regional Council of Kymenlaakso. In this project, we map cyber threats to occupational safety in port logistics. The Cyber Hygiene Handbook is based on interviews conducted in spring 2023 for companies operating in the Port of HaminaKotka.

Authors:
Tuomas Heikkinen and **Vesa Tuomala**



KYMEN LAAKSON LIITTO

XAMK
Kaakkois-Suomen ammattikorkeakoulu