See Yourself in Cyber

A Self-led journey to cyber risks

CYBEREADY

Let's Start →

CYBERREADY

Before you begin:

The goal of this experience is to help you **identify** your main cyber risks, **understand** them, and **minimize** them

#1 Characterize your **workday**

#2 Uncover your **risks**

#3 Discover **real-life stories**

#4 Learn **what to do**

I'm Ready →

First step:

Characterize **your workday**

Next →

Choose a character you relate to:

I receive dozens of **emails** a day

I mostly work with **customers**

I enjoy working in **public places**

I handle **money** transactions

Characterize your **workday**

Find out your **risks**

Discover **real-life stories**

Learn **what to do**

Every day you receive dozens of emails?

Uncover **your risks**

Next →

The Risks

Your intensive use of email makes you especially vulnerable to these forms of fraud:

Phishing

Business-Email-Compromise (BEC)

What Does it Mean? →

Discover real-life stories

People fall victim to these scams every day.
Here are some of their **stories** to help you understand these risks

Next →

“It was one of those days with no time for coffee. **I received an email** from "Human Resources.” In it was a link to a form asking for my details, including my corporate email and password.

During lunch, **I discovered that none of my colleagues were asked to fill out such a form.** Was I phished?”

Next →

"**I got an email** from a customer asking me to help him access his data. He wrote that he was about to sign a deal and needed financial statements fast, **so I shared the confidential information with him**.

Later, when I looked at the email again, I noticed **the email address was misspelled. Even the name had a typo**."

Next →

"**I received an email** from "Danny Monel," my boss. In it, he asked me to **transfer funds to a vendor immediately**, as we were in violation of a contract.
After filling his request promptly, I felt like the greatest employee.

Only later, when I looked again at the email, did I realize that **something there was very wrong**."

Next Step →

And now, for the final step:

Learn What to do 

4 tips on how to reduce your risks

#1 **Review** the sender's email address and verify it's what you expect

#2 **Contact the person who initiated the request** on a separate thread or channel (whenever you're suspicious)

#3 **Hover over links** to verify that URLs point to a known site (on mobile phones, pressing and holding the link will reveal the website address)

#4 **Beware of emails that urge you to act quickly**. These should raise a red flag.

Done →

Working with customers?

Uncover **your risks**

Next →

The Risks

Working with many people (like customer service roles) makes you especially vulnerable to these risks:

Impersonation Fraud

Confidential information sharing

What Does it Mean? →

Discover real-life stories

People fall victim to these scams every day.
Here are some of their **stories** to help you understand these risks

Next →

“**I received an email** from "Ben" from the customers’ accounting requesting some documents for the project I was working on. **So I emailed it**.

It was only when my company got sued that **I discovered there was no Ben on the customer’s payroll**.”

Next →

"**My boss asked me to share the annual revenue spreadsheet** with Michael from finance, **which I did**. A week later, it was in the news.

Turns out I accidentally sent it to a Michael from another company in our space."

Next →

"**A woman called me** crying, asking for her thirteen-year-old son's call log as he was missing. **I felt an immediate need to help** her without burdening her with too many questions.

I only discovered **I had sent the details to a private investigator** investigating a cheating spouse after we got sued."

Next Step →

And now, for the final step:

Learn What to do 

4 tips on how to reduce your risks

#1 **Always Verify** the identity of the person you're conversing with

#2 Before sharing customer-related information, **double check** that the information can explicitly be shared

#3 Share sensitive information **only through designated channels**

#4 Be attentive to the **requester's tone**. If someone tries to pressure you, it is usually a sign of fraud

Done →

Working in public places?

Uncover **your risks**

Next →

The Risks

Working in public places makes you especially vulnerable to these risks:

Laptop theft

Shoulder surfing

Wi-Fi attack

What Does it Mean? →

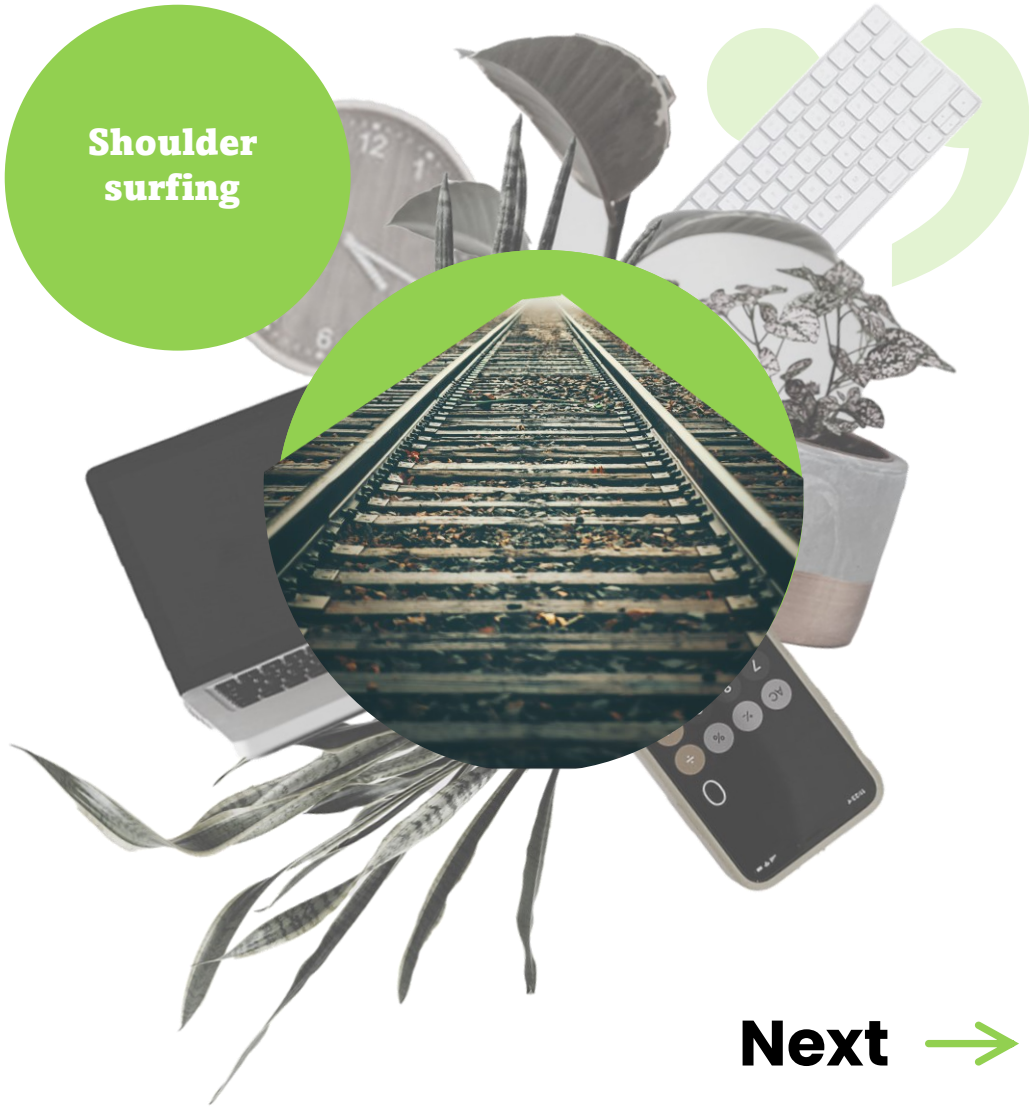
Discover real-life stories

People fall victim to these scams every day.
Here are some of their **stories** to help you understand these risks

Next →

“It was a crowded day on the **train**. Since I had an important report to complete, **I worked on my laptop**. The following day, I came across a Reddit post containing **inside information about our company that was mentioned in my document**.

Is it possible that I was the **leak**?”



Next →

"One day, while **working at a cafe** where I often sit, **I got up** to pick a pastry **and left my laptop unattended for only a moment**.

When I returned, **it was no longer there**."

Next →

“On my way to a client, I had to check some details. **So I connected to the free café Wi-Fi nearby**, checked, and closed it.

Next month, **there was a hack into our system** using my user. I can't shake off the idea that it might have been caused by my use of a rogue Wi-Fi.”

Next Step →

And now, for the final step:

Learn What to do 

3 tips on how to reduce your risks

#1 Always **keep your laptop next to you**. You'd be amazed how many are stolen each year.

#2 **Use only a private internet connection**, never public ones

#3 Ensure that **only you can see the screen** of your laptop and notes

Done →

Handling money transactions?

Uncover **your risks**

Next →

The Risks

Having permission to wire funds makes you vulnerable to these forms of fraud:

Business-Email-Compromise (BEC)

Vendor impersonation fraud

What Does it Mean? →

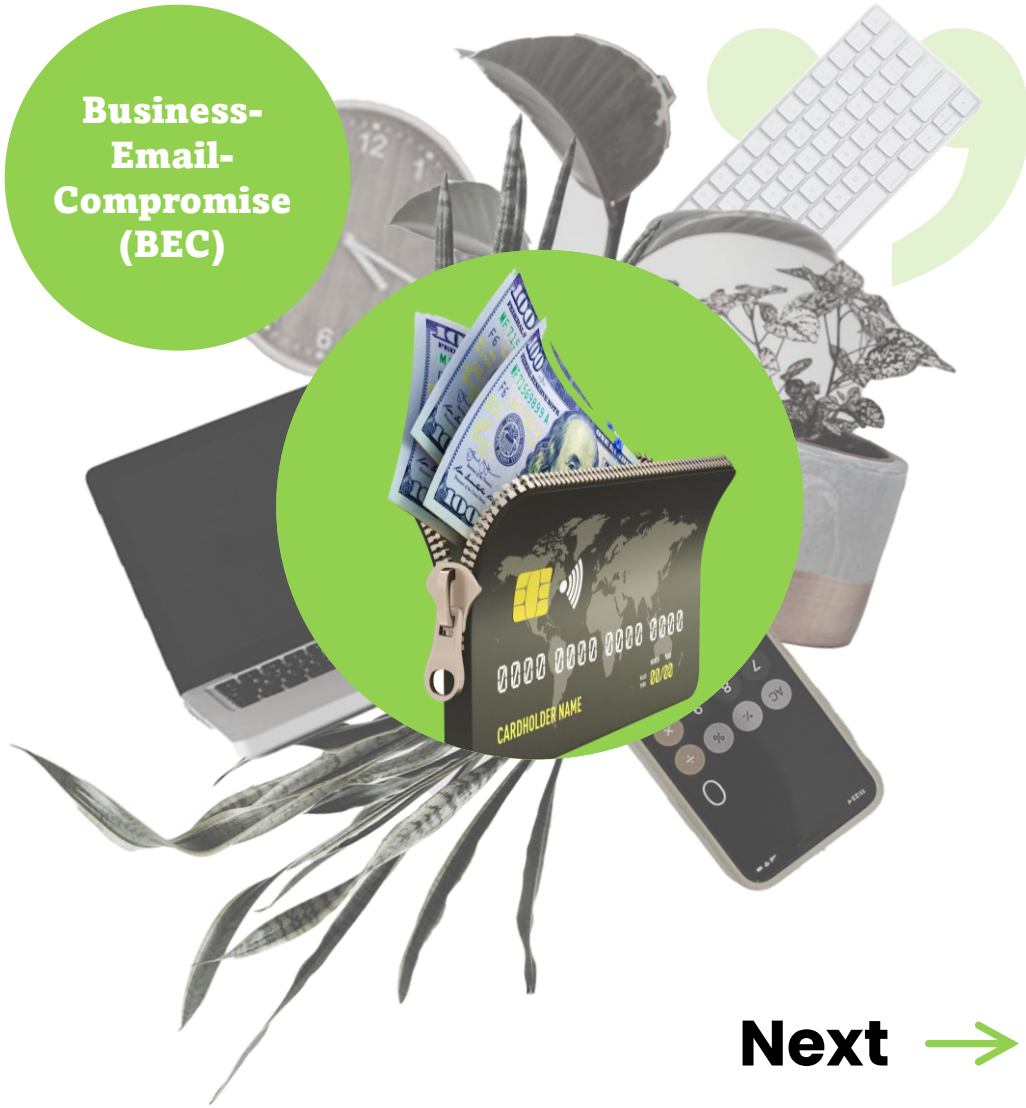
Discover real-life stories

People fall victim to these scams every day.
Here are some of their **stories** to help you understand these risks

Next →

“**I got an email** from my boss telling me to **transfer 17,000 dollars to a new vendor**. He wrote, ‘I'm in a meeting. unable to talk. **Please transfer the money ASAP**’, so I did.

Only a day later, in the office, I realized **he had no idea what I was talking about**.”



Next →

"**I got a mail** from one of our vendors' **newly appointed financial manager** that requested that **future payments** be sent to a different bank account. **So I did it**.

It was a **fraud**, but how could I have known?"

Next →

"**I got an email** from HR with a long thread in it. They asked that I **purchase gift cards** for the new year party. All they needed was their numbers. So I **bought the cards and sent them the numbers**.

As it turns out, it was a fraud, and all the **money was gone**."

Next Step →

And now, for the final step:

Learn What to do 

3 tips on how to reduce your risks

#1 **Check** the sender's email address. If it's different than usual, close the email and contact the presumed sender in a different way

#2 **Verify any change request** of payment method with your usual contact person, face-to-face or by phone

#3 **Slow down**. Hackers try to get people to act quickly so they won't notice alarming signs or consult with others

Done →

Great! You have completed the journey

What would you like to do now?

Explore Another Journey

Finish

Thank you for participating

We hope you enjoyed and gained valuable insight from this experience we built