KYBERX

Cyber Awareness Training

That Actually Changes Behaviors

How to Turn Cyber Awareness Into Your Foundation for Growth.

📅 **Date**: Thursday, 21 August 2025 11am
🕛 **Duration**: 45 minutes

Presenters:

Tamas Balogh - **KYBERX**

Agenda

01 Welcome

02 About KYBERX

03 The 3 cyber habits your team can start using today

04 How modern cyber awareness platforms change behavior

05 Live Q&A

06 Closing

AS SECURE AS THAT.

About KYBERX

KYBERX

Cyber Awareness & Compliance Automation — Built for Growing Teams

We help Baltic businesses build cyber-smart teams and automate compliance using proven platforms and practical support.

01 **AWARENESS**

Train your team to recognize and respond to cyber threats effectively.

- Awareness *Platform Delivery*
- *Fully-managed Awareness Program*
- *Pulse Check / Course Correct / CultureSync*
- *Cyber Escape Room*
- *Monthly Cyber Awareness Pack*

02 **COMPLIANCE**

Simplify your compliance processes and journey with automation, and pass audits and run your cybersecurity program with confidence.

- *Compliance Automation Platform Delivery*
- *Framework Alignment*
- *Controls Identification & Implementation Support*
- *Fully Managed ISMS*

03 **ADVANTAGE**

Combine training and compliance automation with a comprehensive tailored cybersecurity strategy and outsourced cybersecurity management.

KYBERX

Contacts

Based in Latvia.
Serving the Baltics and beyond.

www.kyberx.io

+371 254 240 63

info@kyberx.io

AS SECURE AS THAT.

3 Cyber Habits That Shift Risks

KYBERX

PUBLIC

Habit 1: **Pause. Check. Verify.**

Includes the “Drag to Nowhere” technique.

Pause

Create a micro-break between reading and reacting. Breathe. Look again.

Check

Hover over links (or long-press on mobile); Scan the sender’s email, not just the name; Look for mismatched branding, urgency cues, or strange phrasing.

Verify

Ask the sender directly through a known channel; Call if it feels urgent; Ask a teammate if you’re unsure.

BONUS Technique:

Drag to Nowhere

If you accidentally click but haven’t released — don’t let go. Just drag your mouse or finger to a neutral part of the screen. Let go there. You’ve just dodged a potential breach.

✅ What it is

A simple 3-step habit that helps anyone pause and process messages before reacting — especially under pressure.

✅ Why it works

It teaches people to slow down just enough to notice what’s off… and respond smartly, not emotionally.

- Most click mistakes happen **because of speed** — not ignorance.
- This habit introduces **just enough friction** to catch the red flags.
- It creates **a shared reflex** — *“Pause, Check, Verify”* becomes part of culture.
- “Drag to Nowhere” gives people a **physical safety trick** they’ll never forget.

Flashcard

Habit 1: **Pause. Check. Verify.**

1

PAUSE

Slow down.

2

CHECK

Scan the sender, subject, link & tone.

3

VERIFY

When in doubt — ask.

4

If you click by mistake:

DRAG TO NOWHERE

Habit 2: **Sender, Subject, Link & Tone**

Your instant message scan — fast, teachable, and memorable.

Sung mentally like:
🎶 **Sender, Subject, Link & Tone, Link & Tone…** 🎶

Sender
Who's it from really? Not just the display name → check the full email address. Is the domain strange? Is anything misspelled?

Subject
Ask: Was I expecting this message? If it came with an attachment, was I expecting to receive that? Is it out of character?
If it's vague, emotional, or trying to create panic — slow down.

Link
Hover (or long-press if on mobile) to preview where it actually goes.
If it feels like bait, it probably is.

Tone
Is it pushy? Too casual? Slightly "off"? ..and again: is it out of character?
Messages that feel wrong usually are.

Inspired by:

✅ What it is

A 4-step mental checklist for scanning any message — email, SMS, Teams, Slack, etc. — in seconds.

✅ Why it works

It can help employees spot suspicious patterns even without needing any technical training.

- It creates a **repeatable reflex** for anyone, regardless of role or technical background.
- Easy to teach, easy to remember — **like a song stuck in your head**.
- **Works across all platforms** — not just email.
- Helps teams learn to **recognize patterns, not memorize examples**.

Flashcard

Habit 2: 🎶 Sender, Subject, Link & Tone. 🎶

SENDER

Who sent it?

SUBJECT

Was I expecting it?

LINK

Where does it lead?

TONE

Does it sound off?

Habit 3: **Don’t Just Delete — Report. Everywhere.**

From inbox to Instagram — teach reporting like a reflex.

At Work

Use the “Report Phish” button, forward to IT, or screenshot and share. Even if it’s a false alarm — you’re strengthening your workplace`s defenses.

In Personal Life

Flag scams in Gmail, Outlook, Facebook, Instagram, or SMS. If it seems like something that could affect others — report it to your ISP or national CERT.

In the Family

Teach kids to ask before clicking. Teach parents to screenshot and send when unsure. Turn “Hey, does this look real?” into a habitual conversation.

✅ What it is

Most employees delete suspicious messages — and think they’ve done the right thing. But that deletes the signal your security team needs most.

✅ Why it works

This habit builds the instinct to report threats, not just not to fall for them — across work tools, personal accounts, and even at home.

- Reporting is how your security team gets ahead of threats — **it’s proactive defense**.
- NIS2 requires incident reporting — but **you can’t respond to what you don’t see**.
- Teaching people to report builds a **shared responsibility model** — one that scales far beyond firewalls and workplaces.

Flashcard

Habit 3: **Don’t Just Delete — Report. Everywhere.**

WORK

Report phish, don’t just delete.

PERSONAL

Flag and report across platforms.

FAMILY

Teach others to screenshot + ask.

AS SECURE AS THAT.

How modern awareness platforms change behavior

But 1st: Why Cyber Awareness Matters to You in Latvia

Ministru kabineta noteikumi Nr. 397

Minimālās kiberdrošības prasības

https://tapportals.mk.gov.lv/structuralizer/data/nodes/9f1d8b20-6917-4235-b4db-250e73e94aaa/

Highlights as they relate to cyber user awareness:

- At hiring: **Initial** cybersecurity briefings
- Day-to-day:
  - **Regular** cybersecurity briefings
  - **Emergency** cybersecurity briefings
- Annually: Training content is **reviewed and**, if necessary, **updated**

3.11. Kiberhigiēnas pasākumi

76. Subjekts organizē tā nodarbinātajiem un amatpersonām, kuri ir subjekta IKT resursu un informācijas sistēmu reģistrētie lietotāji, apmācību kiberdrošības jautājumos, izvēloties tādu apmācības veidu un saturu, kas atbilst nodarbināto un amatpersonu profesionālajai sagatavotībai, ņemot vērā viņu izglītību, iepriekšējo apmācību, darba pieredzi un spējas, kā arī subjekta darbības specifiku. Apmācību kopums ietver:
    76.1. subjekta nodarbināto un amatpersonu, kuri lieto IKT resursus un informācijas sistēmas, kiberdrošības instruktāžas, tai skaitā:
        76.1.1. sākotnējās kiberdrošības instruktāžas – ne vēlāk kā viena mēneša laikā no fiziskās personas lietotāja konta reģistrācijas brīža;
        76.1.2. kārtējās kiberdrošības instruktāžas – vismaz reizi kalendāra gadā;
        76.1.3. ārkārtas kiberdrošības instruktāžas – pēc kiberdrošības pārvaldnieka ieskatiem (piemēram, identificējot jaunu risku, ievainojamību vai kiberapdraudējumu, paredzot normatīvo aktu prasību izmaiņas, plānojot vai veicot nozīmīgas izmaiņas IKT infrastruktūrā, programmatūrā vai biznesa procesos);
    76.2. subjekta nodarbināto un amatpersonu IKT personāla apmācības kiberrisku pārvaldības un IKT darbības nepārtrauktības pasākumu efektīvai īstenošanai – vismaz reizi kalendāra gadā. Kiberdrošības pārvaldnieks ir tiesīgs organizēt papildu apmācības, piemēram, identificējot jaunu risku, ievainojamību vai kiberapdraudējumu.
77. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:
    77.1. piešķir fiziskajai personai lietotāja kontu pēc šo noteikumu 76.1.1. apakšpunktā noteiktās sākotnējās kiberdrošības instruktāžas;
    77.2. liedz fiziskajai personai piekļuvi tās lietotāja kontam, ja tai nav veikta šo noteikumu 76.1.2. apakšpunktā noteiktā ikgadējā kiberdrošības instruktāža;
    77.3. organizē ārpakalpojuma sniedzēja darbiniekiem, kas ir iesaistīti līguma izpildē, kiberdrošības instruktāžas pirms līguma izpildes uzsākšanas.
78. Subjekts nodrošina, ka apmācību saturs tiek pārskatīts un nepieciešamības gadījumā aktualizēts vismaz reizi gadā vai mainoties apstākļiem (piemēram, izceļoties jauniem kiberapdraudējumiem, mainoties kiberriska līmenim, notiekot kiberincidentam).
79. Subjekts nodrošina, ka visiem tā nodarbinātajiem un amatpersonām, kas lieto subjekta IKT resursus un informācijas sistēmas, ir pieejami aktuālie kiberdrošības instruktāžu materiāli.
80. Subjekts uzskaita organizētās kiberdrošības instruktāžas un novērtē nodarbināto un amatpersonu, kuri lieto subjekta IKT resursus un informācijas sistēmas, zināšanas kiberdrošības jautājumos un īstenoto kiberdrošības instruktāžu efektivitāti.

How Modern Cyber Awareness Platforms Change Behavior

And help you keep your organisation safe and compliant

Tailored to the individual

When you meet the employees where they are, they will have a lot more rewarding learning experience, and most importantly a successful one.

Micro-learning

Instead of unloading all the cyber wisdom possible once a year, it is a much better approach to provide the employees regular bite-sized training helping them build cyber-smart habits that will stick.

Dynamic content

We believe that awareness training must be kept up-to-date to ensure that employees are not only ready for the long-standing techniques of cyber criminals, but all the latest and emerging tricks, too.

A platform that is aware

Localisation is important, and that means not only language support, but also ensuring the platforms and the training fit well into the context where the organisations operate.

Let`s take a quick look! 👀

Next Steps

Share the learnings

Help your Teams and family to be better equipped to face today`s cyber threats by sharing today`s teaching points.

Start Conversations

Use the free resource to start conversations, normalize asking questions and assess where your awareness program is at today.

Book a Consultation

Free consultation to discuss your needs and requirements & to help you find the right next steps for your user awareness program.

Follow us on social media for more tips

Find us on LinkedIn:

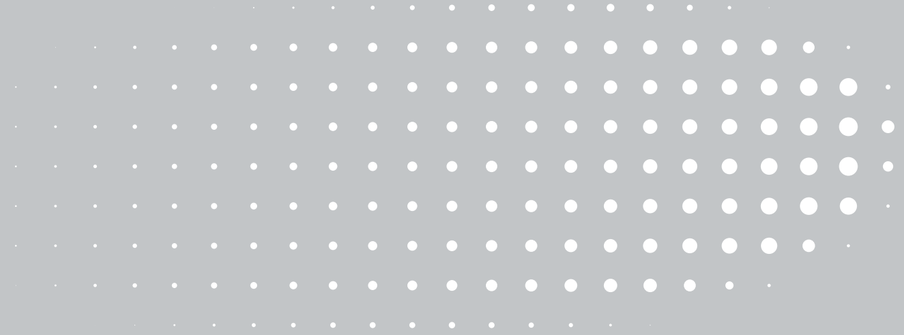
- linkedin.com/in/tamasbalogh/
- linkedin.com/company/kyberx/

AS SECURE AS THAT.

Free Resources,
Quick Survey
Live Q&A

Please don`t forget to:

- Download your free resource
- Complete the quick survey
- Ask your questions in the chat



💡 **Remember!**

User Awareness isn’t a one-off project —
it’s an ongoing process:

- Start small,
- prioritise impact,
- and keep improving.

The 3 cyber habits and the handout we shared are a good start to begin the conversations.

KYBERX

Thank You!