



BEING-WISE
CA22104

COST ACTION CA22104
Behavioral Next Generation in Wireless
Networks for Cyber Security
(BEING-WISE)



cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY



Funded by
the European Union

This educational material is based upon work from COST Action BEING-WISE CA22104, supported by COST (European Cooperation in Science and Technology). COST (European Cooperation in Science and Technology) is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career and innovation.
www.cost.eu

BEING-WISER

Your Mind's Security Map

The way you **think** about threats shapes every click you make. Most people never notice the lens.





THE INVISIBLE LENS

You're Never Browsing Alone

Every time you go online, an **invisible mental map** shapes what you notice, what you ignore, and what you click. You don't see it, but attackers count on it.

THE PERCEPTION GAP

Same Moment. Two Realities.

What You Think

- "Just a warning popup"
- "Probably nothing"
- "The padlock is there"

What's Happening

- Active credential theft
- Data interception in progress
- Certificate spoofing attack

The gap between perception and reality is the most exploited vulnerability online.

The Coffee Shop Wi-Fi

You Think

"Free Wi-Fi = safe internet." The café wouldn't offer something dangerous.

The Reality

Anyone can create a fake hotspot called "CoffeeShop_Free" in minutes. Your passwords travel through open air.



Physical ≠ Digital. Wireless = Exposed.

The Security Warning

You Think

"Just a glitch." I'll click Proceed Anyway, like always.

The Reality

Some warnings signal active **man-in-the-middle attacks**. Not all warnings are equal, but your brain treats them the same.

📌 **Warning Fatigue** is a feature attackers rely on.

The "Strong" Password

You Think

"Nobody would guess

P@ssw0rd123!"

I replaced letters. I'm safe.

The Reality

Attackers don't *guess*. **Algorithms** try billions of combinations per second and common substitutions are first on the list.



Human Burglar vs. Machine-Speed Attacks

The Friendly Email

You Think

"I can spot a scam."

Bad grammar.

Obvious logos. Easy to tell.

The Reality

AI-generated phishing is **pixel-perfect**. Your 2010 instincts don't protect you in 2025.

Today's attacks exploit **trust**, not carelessness.



Scams Look Obvious until they don't.

Trust is the target.

MENTAL MODEL #5

The App Permissions

You Think

"It's app-store approved." If it were dangerous, someone would have caught it.

The Reality

A flashlight app needs **only a camera flash.** Excessive permissions are a data strategy. The marketplace doesn't protect you, **you do.**



Gatekeeper Trust: You are the last gatekeeper.



5 Ways Your Brain Maps Cyber Risk

We borrow real-world concepts to understand digital threats. Each one shapes and limits how you respond.



Physical Security

"Lock the door"

The internet is like a house.



Criminal Behavior

"Catch the thief"

Hackers are criminals; let someone else handle it.



Medical Infection

"Cure the virus"

Install antivirus and recover.



Warfare

"Defend the line"

Build firewalls; stay vigilant.



Market Failure

"Regulate it"

Companies should protect you.



NO MODEL IS COMPLETE

Every Model Has a Blind Spot



Physical

Misses automated, invisible attacks



Medical

Misses social engineering



Warfare

Misses insider threats

The most resilient people **combine models**. Which one do *you* default to?

Experts vs. Everyday Users

Expert Thinking

- Threats are continuous, not binary
- Security is a process, not a product
- Every warning carries a different risk
- Trust must be verified at every layer

Most People Think

- You're either safe or hacked
- Antivirus = fully protected
- All warnings look the same
- Known brands are always trustworthy

Closing this gap means speaking the right **cognitive language**, not the expert one.

UPGRADE YOUR MIND

4 Habits That Actually Protect You



Pause Before You Proceed

When you dismiss a warning, ask: "**What model am I using? What am I missing?**"



Think in Layers

Security is not one lock.
Device → Network → App → Behavior. Each layer has its own risks.



Retire Outdated Assumptions

Threats evolve faster than mental maps. Follow credible sources. Update what you know.



Default to Skepticism

Too urgent? Too familiar?
Too convenient? It may be engineered to exploit your trust. **Verify first.**

START THE CONVERSATION

3 Questions Worth Asking Out Loud

1 Which of the 5 models is yours?

Your default lens shapes every decision you make online.

2 When did your model fail you?

Think of a moment you clicked, shared, or ignored something you shouldn't have.

3 How would you explain cyber risk to a child?

The metaphor you choose reveals your dominant mental model.

BEING-WISER

The Best Firewall is an Upgraded Mind.

The gap between what we *think* is happening and what *actually* happens online is the most exploited vulnerability in cybersecurity today.



Know your model



Combine models



See your blind spots