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

BEİNG-WISER

Why Smart People Still Make Unsafe Online Choices

It's not carelessness. It's a **mental model** problem.
Swipe to find out why.

WHAT YOU'LL LEARN

By the end of this carousel, you'll understand:

01

What a mental model is

The invisible map in your head that shapes every click.

02

Why it matters in cybersecurity

Your assumptions are your first line of defense or weakness.

03

How weak models create real risk

Familiar-looking ≠ safe. We'll show you why.

04

What better awareness looks like

Simple shifts that make your online decisions sharper.

CHECK YOURSELF

Have you ever thought any of these?

"A padlock means the whole site is safe."

SSL only encrypts data it doesn't verify who owns the site.

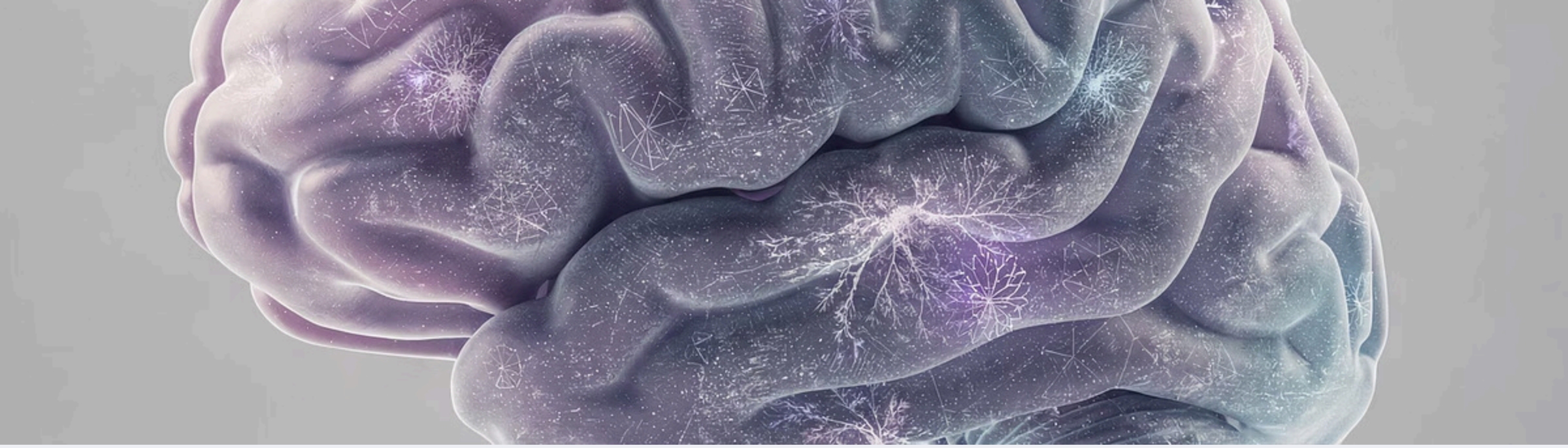
"A familiar brand can't be phishing."

Attackers frequently impersonate trusted brands to exploit your confidence.

"If an app is popular, my data is protected."

Popularity does not guarantee strong privacy practices or secure data handling.

These are **mental models in action** and every one of them is incomplete.



CORE CONCEPT

So... What Is a Mental Model?

> **A mental model is the internal explanation you use to predict how a system works even when that explanation is wrong.**

The gap between these two sides is where most security mistakes happen.

WHY IT MATTERS

Mental Models Shape Every Security Decision You Make

Users don't make security choices based on facts alone — they rely on:

Past Habits

"I've done this before and nothing bad happened."

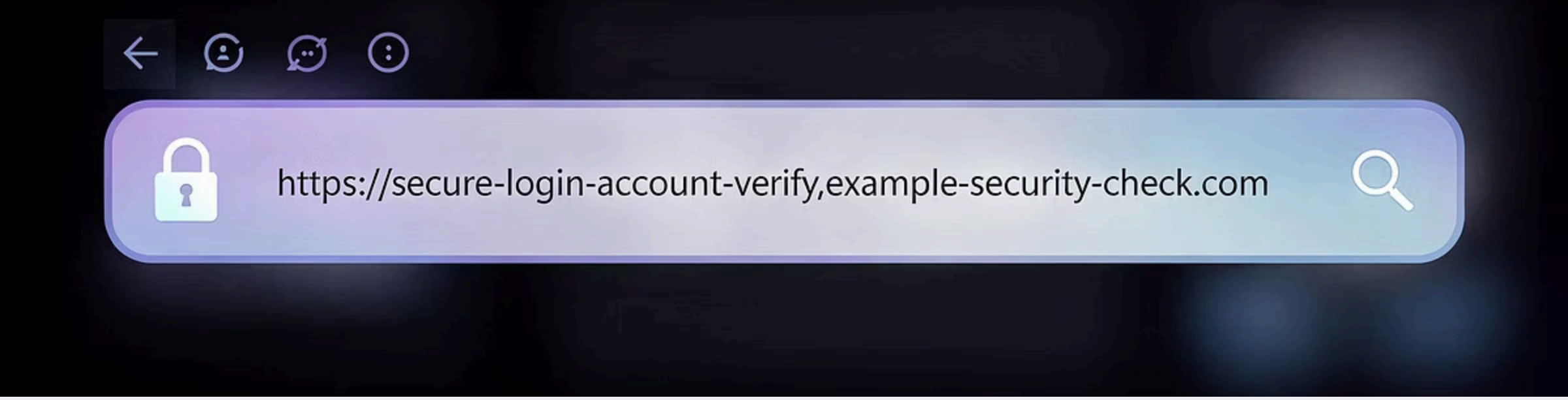
Visual Cues

Logos, colors, and design feel "official."

Familiar Analogies

"It works like a bank, so it must be as secure as one."

When these mental shortcuts are wrong, **risky behavior follows automatically**.



REAL EXAMPLE

The Login Page Trap

A user sees a familiar logo and a lock icon. Their mental model says: **"Looks professional. Must be safe."**

→ **Is the URL exactly right?**

One wrong letter hides in plain sight.

→ **Why is this login appearing now?**

Urgency is a manipulation tactic.

→ **Was this request expected?**

Legitimate services rarely surprise you.

Good cybersecurity = **evidence-based trust**, not visual familiarity.

QUICK CHECK

Which thought reflects a safer mental model?

Pause here and choose before swiping.

A

"This looks familiar, so it's probably safe."

B

"This asks for sensitive info, I should verify before trusting it."

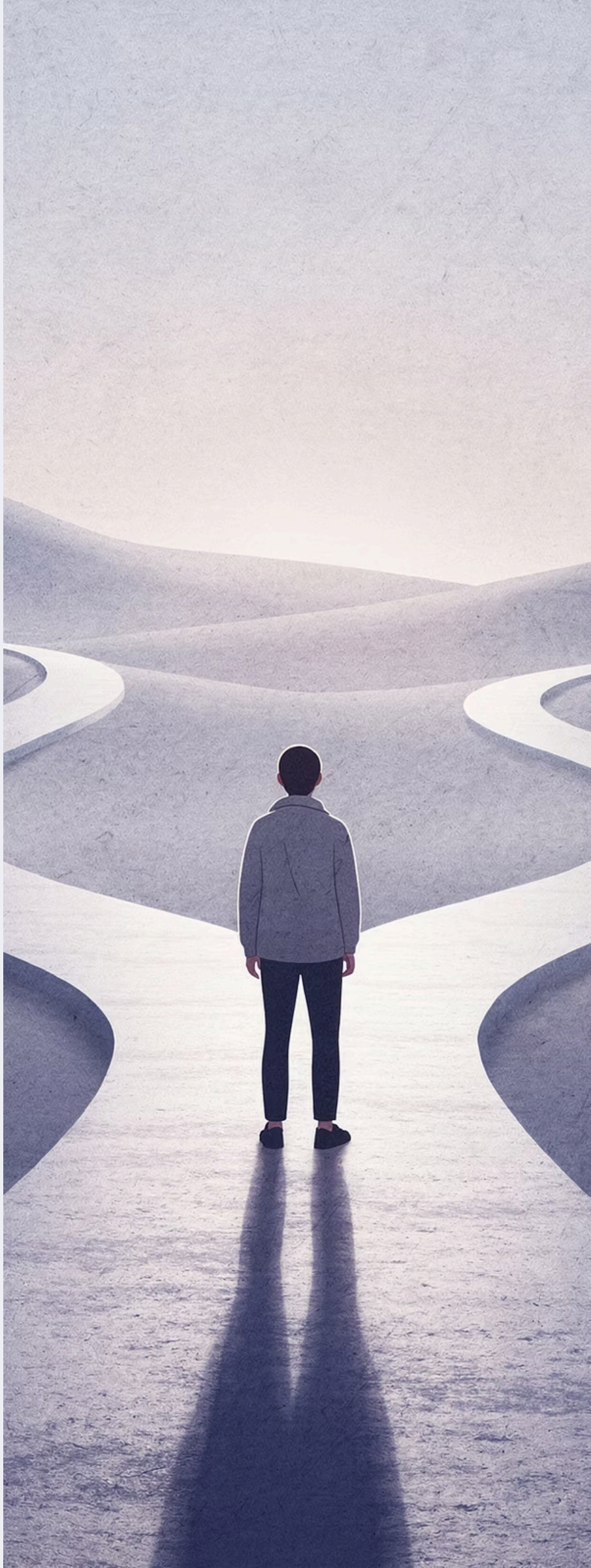
Your instinct reveals your current mental model. No wrong answers, just honest ones.

❌ OLD THİNKİNG

Does this look safe?

✅ BETTER QUESTİON

What makes this trustworthy?



ANSWER

The Answer Is B, Here's Why:

Safer mental models are built on **verification**, not appearance. Before trusting any system, run this quick check:

1

What is this asking me to do?

Name the action clearly before you take it.

2

What proof do I have it's genuine?

Look beyond logos, **check URLs, sender, context.**

3

What could go wrong if I'm wrong?

A one-second pause can prevent a serious breach.

KEY TAKEAWAY

Better Cybersecurity Starts With Better Mental Models

For Users

Replace assumptions with **curiosity** and **verification** habits.

For Designers

Build interfaces that match how people actually think.

For Educators

Correct false beliefs, don't just add more rules.