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 AWARENESS SERIES

Feeling Safe is Not the Same as Being Safe

Your confidence online might be your biggest vulnerability.
Scroll to find out why.

WHAT YOU'LL LEARN

By the end of this carousel, you'll be able to tell the difference between feeling protected and actually being protected.

01

Recognize false security signals

Identify what makes you feel safe — even when you're not.

02

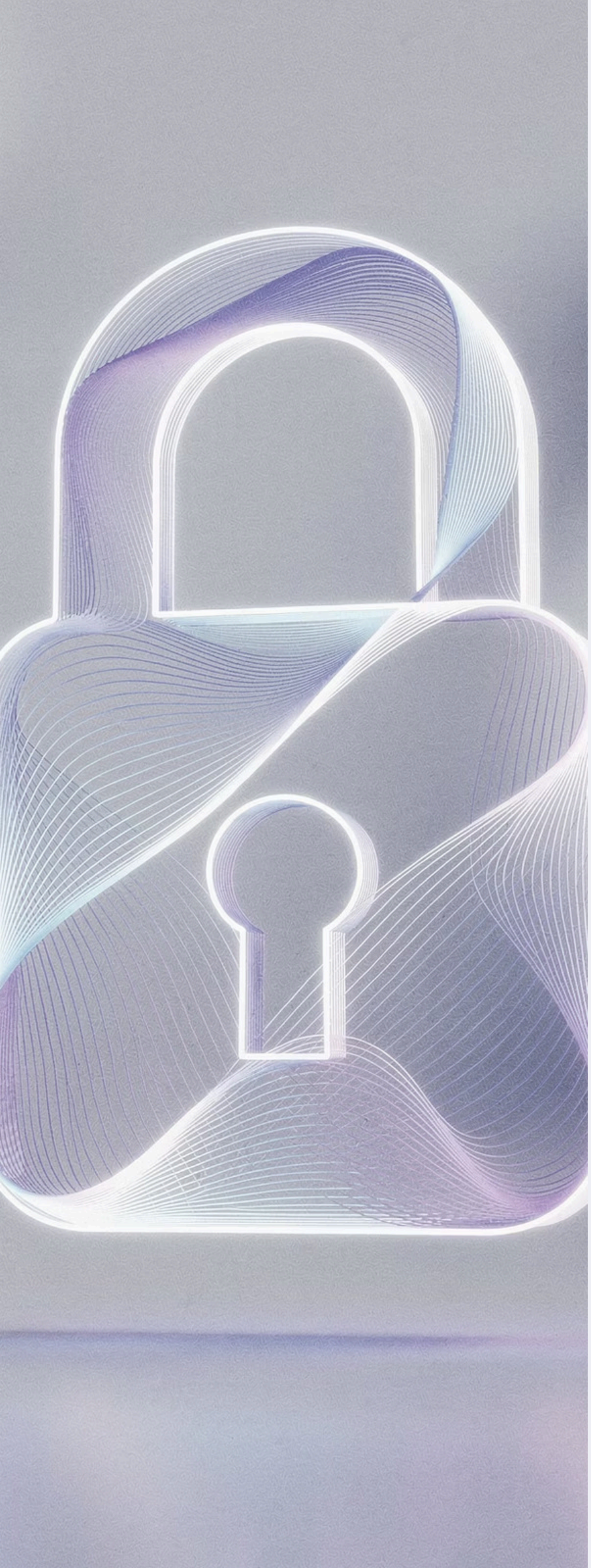
Understand the comfort trap

Learn why familiarity and confidence can mislead your judgment.

03

Apply real risk-checking

Replace assumptions with evidence-based decisions.



SOUND FAMILIAR?

You've used this site a hundred times. It feels totally safe.

1	**"I know this platform."** Familiarity feels like protection but trust built on habit isn't the same as verified security.
2	**"Everyone uses it."** Popularity signals legitimacy in our minds even when risks are widespread or hidden.

CORE CONCEPT

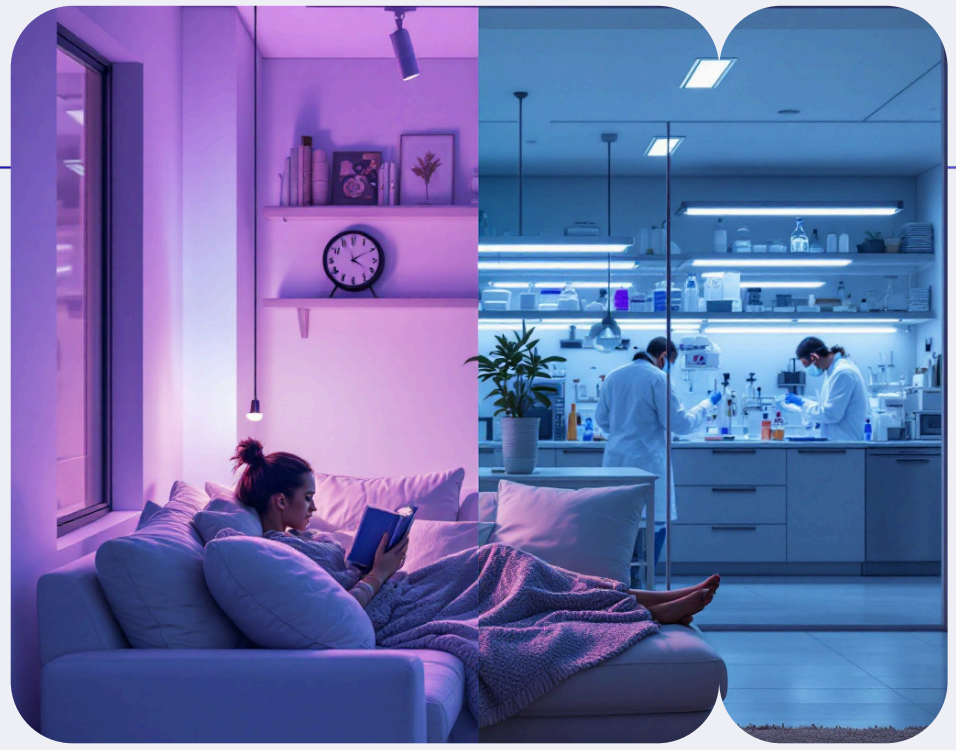
What Is False Security?

> "False security happens when you **feel protected** but the real risk is still present and unaddressed."

It's the gap between your emotional comfort and your actual level of protection. That gap is where harm happens.

Comfort

Feeling safe while risks remain unaddressed



Evidence

Verified risks and assessed protections in place

WHAT CREATES FALSE SECURITY?

5 Things That Make You Feel Safe (But Aren't Proof)

Polished Design

A beautiful, professional-looking interface signals trust but scammers invest in design too.

Routine & Familiarity

Repeating an action without incident doesn't mean the risk isn't there.

Popularity

"Millions use it" doesn't mean millions are protected.

Perceived Control

Feeling in control of your settings ≠ being immune to risk.

Digital Confidence

Tech-savvy users are not automatically safer, **overconfidence is its own vulnerability.**

DEEP DİVE

The Familiarity Bias

Our brains are wired to trust what we recognize. When something looks familiar or resembles something safe, we lower our guard automatically, often unconsciously.

The bias says:

"I've seen this before. It must be fine."

The reality is:

Phishing sites mimic trusted brands. Scammers copy familiar formats. Familiarity is not evidence.

SCIENCE BEHIND IT

Skill vs. Accuracy

Research shows that perceived control and digital skills can motivate action but they can also lead to **overconfidence** when not paired with accurate risk judgment.

Digital Skill

Knowing how to use technology efficiently and navigate digital spaces.

≠

These are not the same thing.

Risk Accuracy

Correctly estimating **how likely** a threat is and **how severe** it could be.

A skilled driver can still underestimate black ice. A skilled user can still underestimate a targeted attack.

FOR PARENTS

When Control Feels Like Protection

Parents who feel confident managing their child's online activity may reduce caution assuming control equals safety. But **perceived control** and **actual risk reduction** are two different things.

→ **Likelihood matters**

How probable is it that harm will occur in this context?

→ **Severity matters**

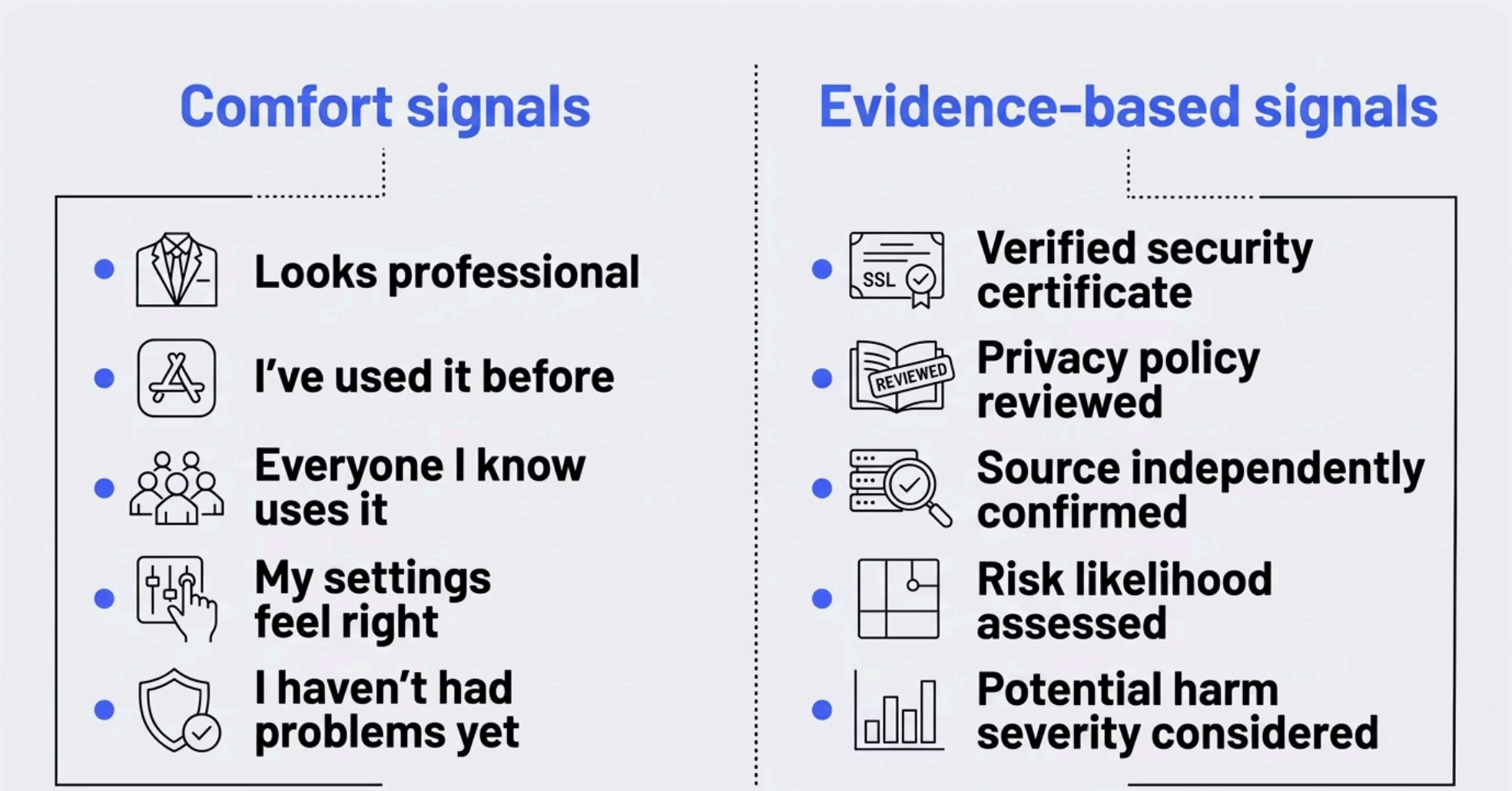
If harm does occur, how serious would the impact be?

→ **Both must be assessed separately**

Feeling in control doesn't answer either question on its own.

COMFORT VS. EVIDENCE

How to Tell Them Apart



Comfort is a feeling. Evidence is a fact. Safe decisions require the second one.

QUICK SCENARIO

What Would You Do?

> You receive a message from a platform you use daily. It asks you to confirm your login, **the page looks exactly like the real site**. You've done this before. It feels totally normal.

Before you click ask yourself:

1

Did I initiate this?

Real platforms rarely ask you to re-login unprompted.

2

Can I verify the URL?

Check the address bar not just the logo or design.

3

Is my feeling based on evidence?

Comfort is not confirmation. Pause before you act.

PRACTICAL TOOLKIT

The 3-Question Risk Check

Before trusting any online interaction, run it through these three questions. It takes under 60 seconds.

Can I verify this independently?

Go directly to the official source, not through a link you were sent.

What's the realistic worst case?

Consider severity: if this goes wrong, how bad could it actually be?

Is my trust based on evidence or habit?

Name one concrete reason -not a feeling- that this is safe.

REMEMBER THIS

Feeling safe is not proof of safety.

Comfort, familiarity, and confidence are signals worth noticing but they are not substitutes for verification. Real protection comes from evidence, not assumptions.

> **What gives people the biggest false sense of safety online?**

Share this carousel with someone who could use a reminder.