



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



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

You trust the Wi-Fi. But do you know who you're trusting?

The invisible risk is real.

Every day, millions connect to public Wi-Fi without a second thought. This carousel will change how you think about that habit.

Keep reading

BEING-WISER SERIES

What You'll Learn

Why public Wi-Fi can be risky

Even when it looks completely normal and familiar.

Why familiar-looking networks can still be unsafe

Official names and real locations don't guarantee security.

How to protect yourself better

Simple, practical habits, no tech expertise required.

The goal isn't to make you paranoid. It's to make you **more thoughtful before you connect.**

SOUND FAMILIAR?

We Connect Everywhere

Train stations, campuses, event venues; connecting feels routine. **And that routine is exactly where caution fades.**

Airport

Waiting for your flight? Wi-Fi is on before your bag hits the floor.

Café

Order a coffee, ask for the password or just pick the strongest signal.

Hotel

The room Wi-Fi feels private. But it's still a shared public network.

What Is Public Wi-Fi, Really?

Public Wi-Fi is a network shared by many users -- in a public or semi-public space. You often can't see who controls it, how it's secured, or whether the one you joined is even the real one.

Shared by many

Every device on that network is a neighbor you didn't choose.

Limited visibility

You can't verify who set it up or how traffic is handled.

Lookalike risk

A fake network with the same name is almost impossible to distinguish by eye.



WHY IT MATTERS

It Feels Normal. That's the Problem.



Fake hotspots look identical

"Airport Free Wifi" and "Airport_Free_Wifi" look the same to most users.



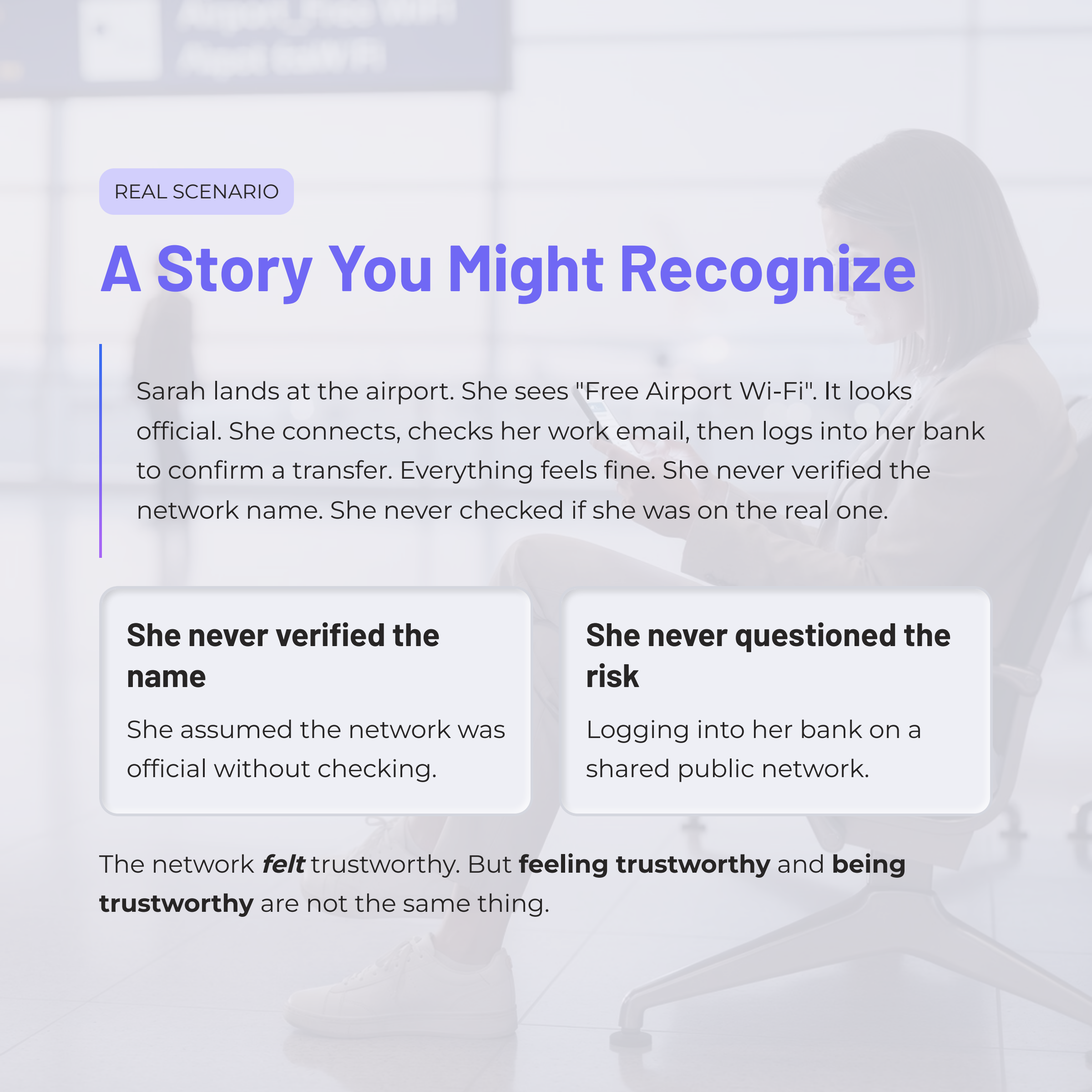
Unencrypted traffic is real

On poorly secured networks, data can travel without protection.



Routine lowers your guard

When something feels familiar, critical thinking quietly switches off.

A woman with long dark hair is sitting in a grey airport-style chair, looking down at her smartphone. The background is a blurred airport terminal with large windows and other people in the distance.

REAL SCENARIO

A Story You Might Recognize

Sarah lands at the airport. She sees "Free Airport Wi-Fi". It looks official. She connects, checks her work email, then logs into her bank to confirm a transfer. Everything feels fine. She never verified the network name. She never checked if she was on the real one.

She never verified the name

She assumed the network was official without checking.

She never questioned the risk

Logging into her bank on a shared public network.

The network ***felt*** trustworthy. But **feeling trustworthy** and **being trustworthy** are not the same thing.

QUICK CHECK

Would You Still Connect?

Log into your bank account?

On a network shared with dozens of strangers?

Open your work email?

With sensitive documents and client data inside?

Enter payment details?

On a free Wi-Fi you picked because the signal was strongest?

The issue isn't fear. It's this: **the gap between how safe it feels and how certain you can be.**

Before You Connect: 5 Questions

1

Do I really need this network?

Mobile data may be a safer choice for sensitive tasks.

2

Is the network name verified?

Ask staff for the exact, official name — don't guess.

3

Am I doing something sensitive?

Banking, work email, passwords — save these for trusted connections.

4

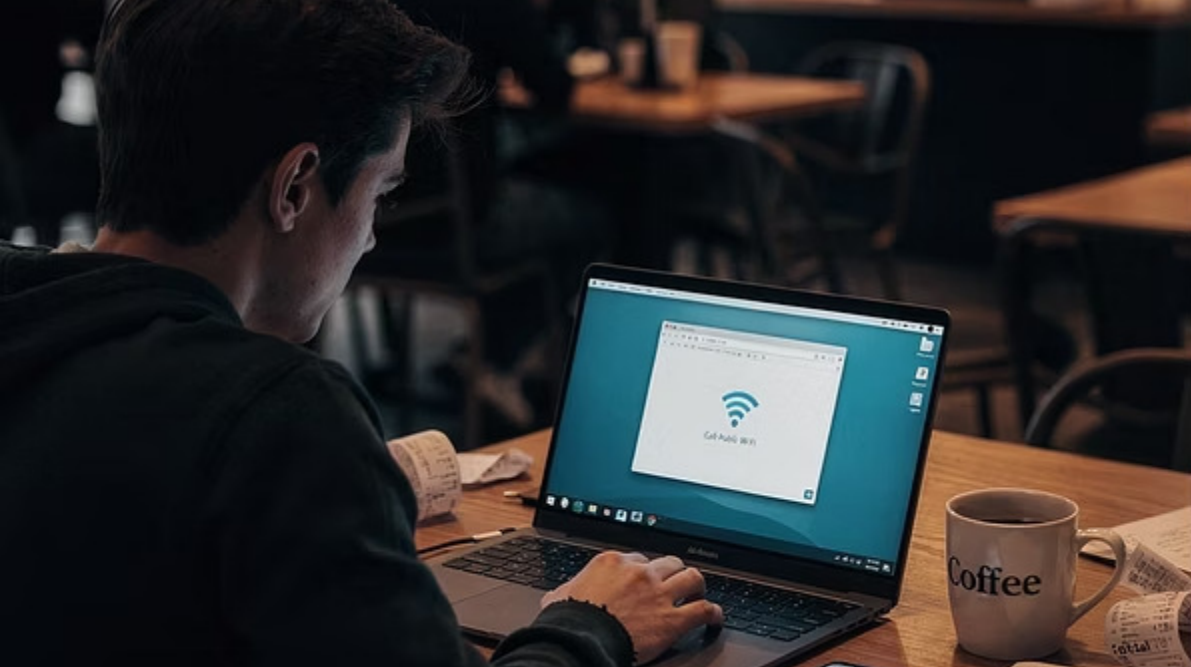
Can I use a trusted hotspot instead?

Your phone's personal hotspot is far more controllable.

5

Is my device protected?

HTTPS, a VPN, and auto-connect off all reduce your exposure.



SAFER ALTERNATIVES

You Have Options



Mobile Data

Your personal data connection. No shared risk, no unknown operator.



Personal Hotspot

Share your phone's connection with your laptop. You control it entirely.



VPN Protection

A VPN encrypts your traffic even on unsecured public networks.



**"Free Wi-Fi is easy to use.
That doesn't mean it's safe to trust."**

A familiar network name is not proof of security. Convenience is not protection. The most important upgrade you can make costs nothing, **it's the habit of pausing before you connect.**

❏ What makes people trust public Wi-Fi too quickly?