Your coffee shop Wi-Fi could be your biggest security risk.

Sounds dramatic?

It happens *every day.*

DIGITAL GUIDANCE

Hannah runs a small marketing agency.

One morning, she grabs her laptop and heads to her favorite coffee shop to get some work done.

DIGITAL GUIDANCE

She connects to the free Wi-Fi.

No password needed.

Perfect for getting through her inbox while sipping a flat white.

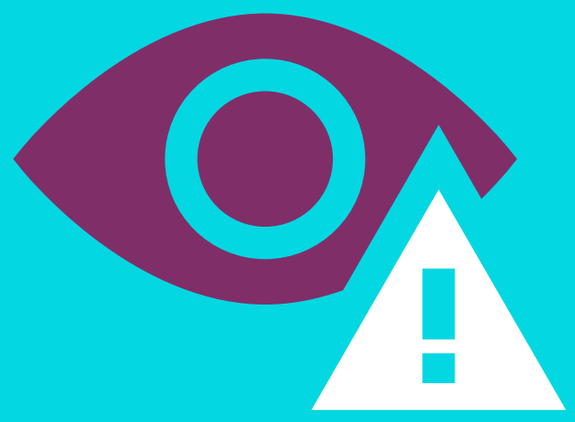
DIGITAL GUIDANCE

But here's the problem...

Someone else in that coffee shop is also "working".

Only they're not sending emails. They're watching Hannah's online traffic.

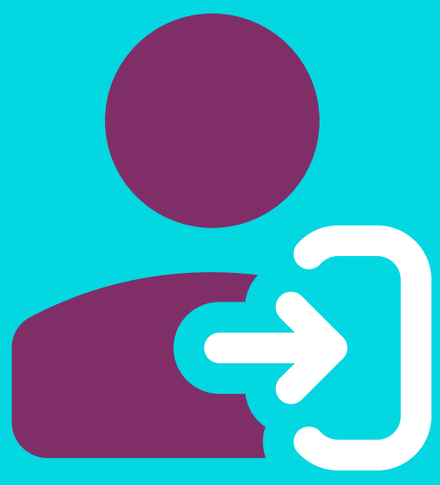
DIGITAL GUIDANCE



That “free” Wi-Fi?

It’s open to everyone, including hackers who can see unprotected data being sent and received.

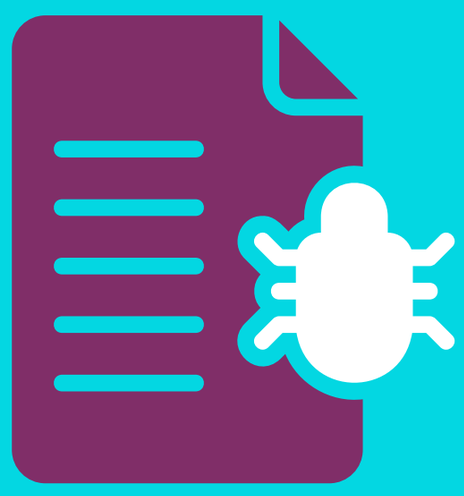
DIGITAL GUIDANCE



They capture Hannah’s login details for her cloud storage and email account.

No alerts.
No warning signs.

DIGITAL GUIDANCE



Later that day a strange file appears on the office server.

Then systems start locking up.

DIGITAL GUIDANCE

Hannah's business has just been hit with ransomware.

All because of that one insecure coffee shop connection.

DIGITAL GUIDANCE

Here's what she *should* have done:

- **Used her phone's hotspot instead of public Wi-Fi**
- **Enabled multi-factor authentication everywhere**

DIGITAL GUIDANCE

Public Wi-Fi isn't always bad, but it's *never* private.

If your team works remotely, they need to know that too.

DIGITAL GUIDANCE

Next time you see that “Free Wi-Fi” sign, ask yourself:

“Is this latte worth a data breach?”

DIGITAL GUIDANCE

Need help keeping remote work secure?

Get in touch.

DIGITAL GUIDANCE