7 Misconceptions of Security Awareness Training

1 Cybersecurity Awareness Training is Boring and a Waste of Time

Yes, 60 minute compliance videos once a year are boring and a waste of time.

This type of training is not:

- Short
- Engaging
- Related to your job role
- Relevant to current threats
- Told like a story

Which one sounds like a bigger waste of time?

5 minute training x 12 months = 1 hour/year

VS

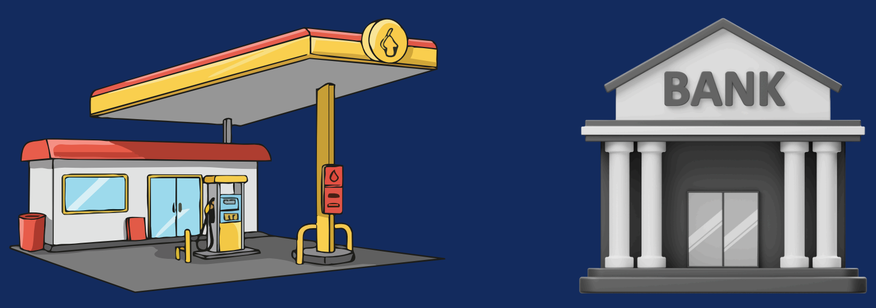
100 days of recovering from a breach

2 We Just Need to Meet Compliance Requirements

Compliance is where you start, not stop. It usually only requires training once per year (that no one likes or pays attention to). It doesn't mean you're more secure, it just means you've checked a box.

Annual training is like studying in school just to pass a test and then forgetting everything over summer break.

Which is more likely to get robbed?



(Hint: The smaller one with less security)

3 Our Business Is Too Small to Get Attacked

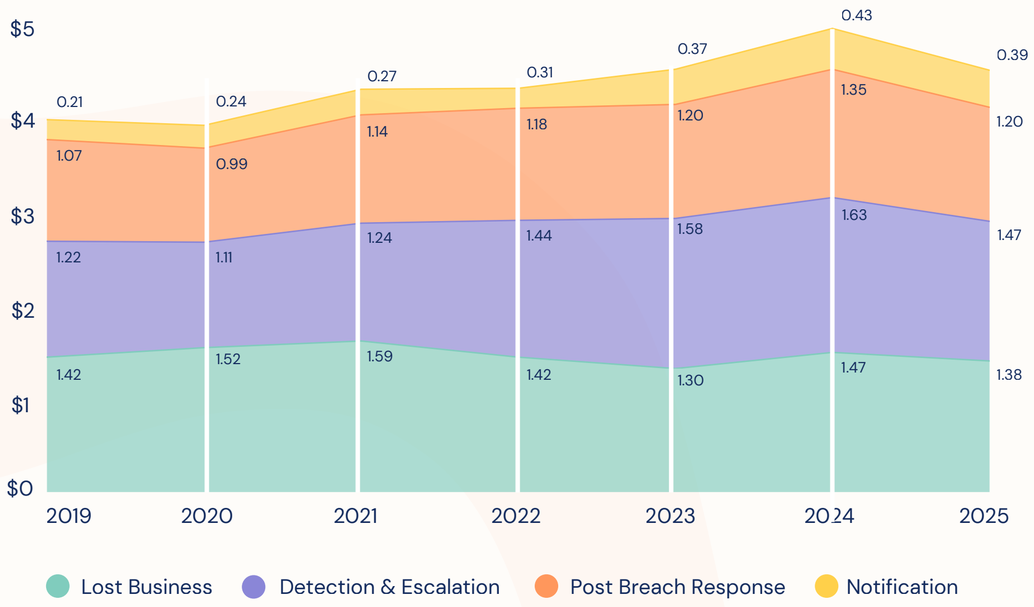
SMBs are the most likely targets because they are often the path of least resistance.

46%

of all cyber breaches impact businesses with less than 1,000 people
SecureWorld

4 It's Too Expensive

Average cost of a data breach measured in millions of USD



IBM: Cost of a Data Breach Report 2024 & 2025

5 Our Employees Aren't Dumb

It's not all about intelligence. It's about habits.

71% of surveyed users said they took a risky action in 2024

96% of users knew they were doing something risky

Your 3 biggest human threats:

Executives & Leadership

New Employees

Untrained Employees

6 We Already Have Security Tools

Tools aren't foolproof.

Human error is still the **#1** cause of breaches.

Phishing is the...

2nd most prevalent cyber attack

3rd most costly cyber attack *(at an avg of $4.88M)*

IBM: Cost of a Data Breach Report 2024

7 Security Awareness Training Doesn't Reduce Risk

Clients have **reduced phishing simulation click rates by as much as 70%** since starting SAT. This means they're effectively reducing the risk of falling for a real phishing threat. Organizations frequently see:

- Lower phishing click rates
- Higher phishing reporting rates
- Faster incident detection
- Improved security habits

Phin: CCB Technology Case Study

Learn more at **phinsecurity.com**

PHIN