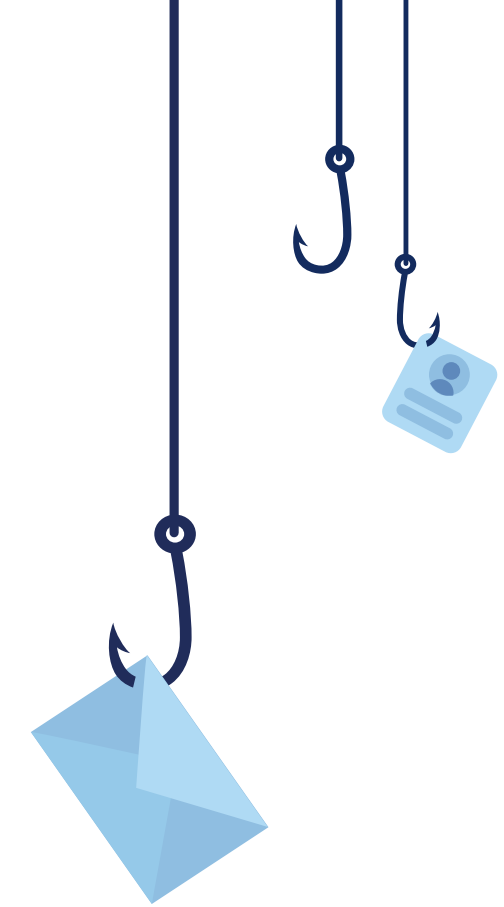


Why Invest in Security Awareness Training?

Statistically Speaking

AGENDA



01.

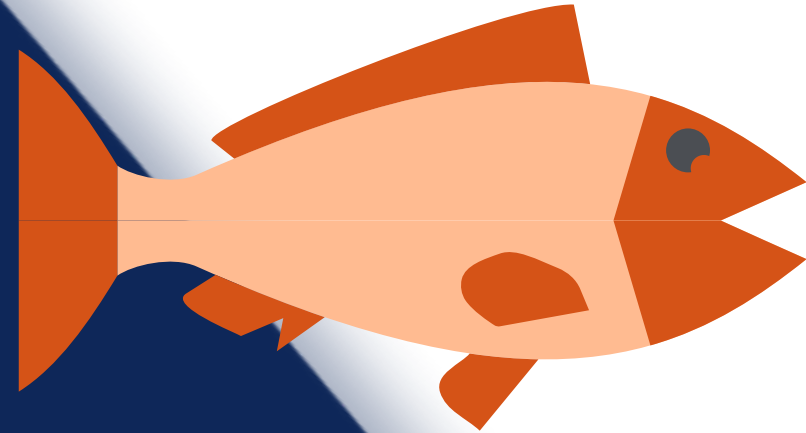
Top excuses for not investing in cybersecurity

02.

The truth behind these excuses

03.

Why invest in Security Awareness Training?



Top Excuses for Not Investing in Cybersecurity

My business is too small to be targeted in a cyberattack



Cybersecurity is too expensive



Cybersecurity is a productivity blocker



Cybersecurity is common sense and doesn't require training



Once a year security awareness training is enough



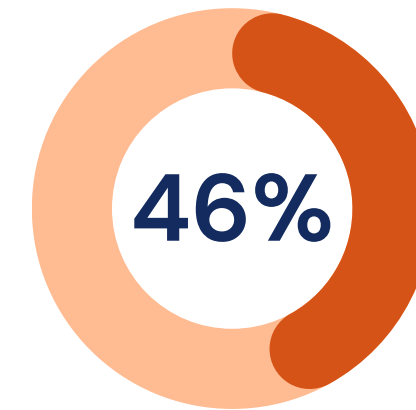
These **excuses** are
hurting your business.

Here's how



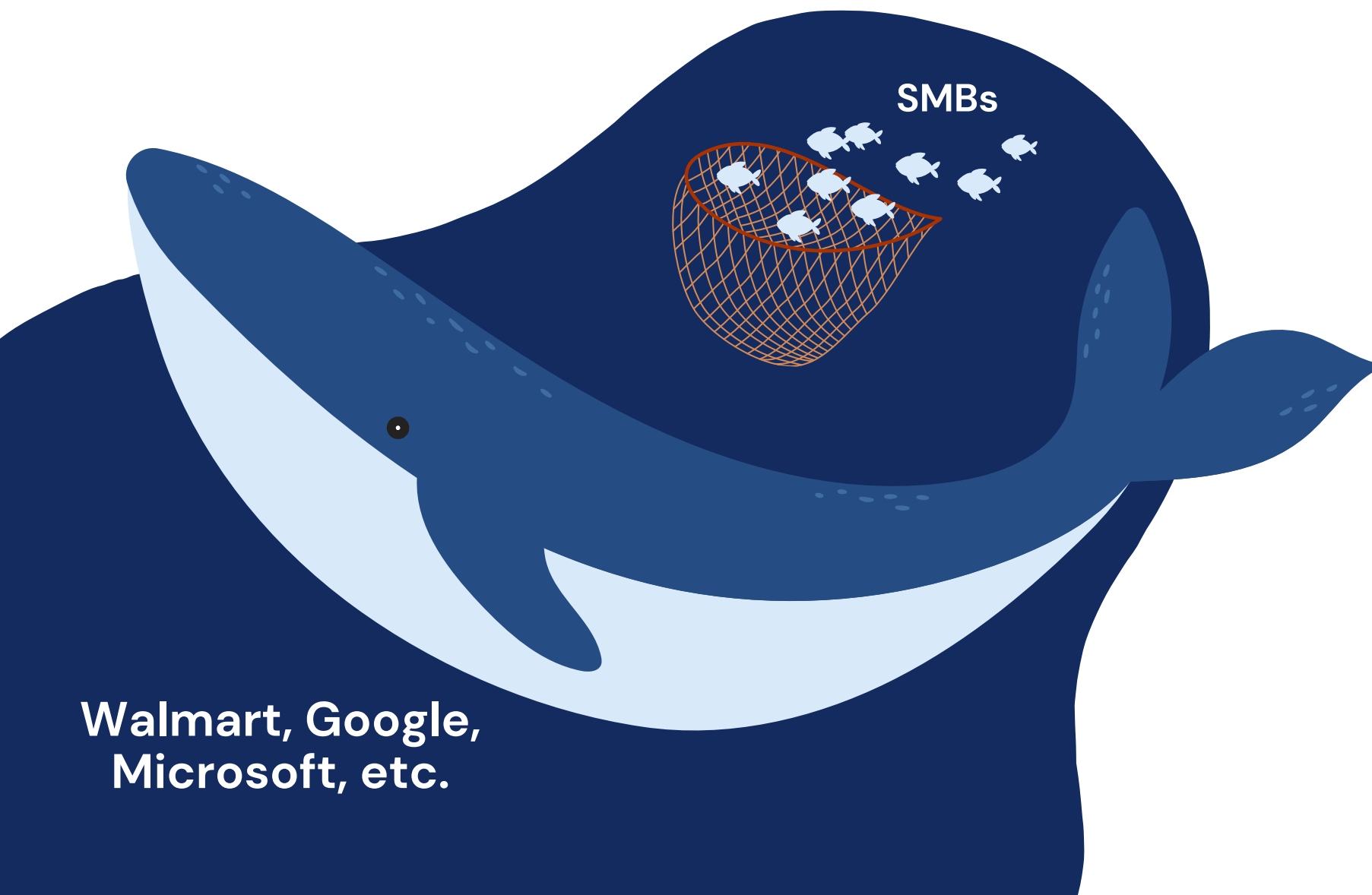
1 No business is too small for a cyberattack

If cyber criminals will go after individuals making less than \$50,000 per year, what makes you think they won't go after your small business?



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

[SecureWorld](#)

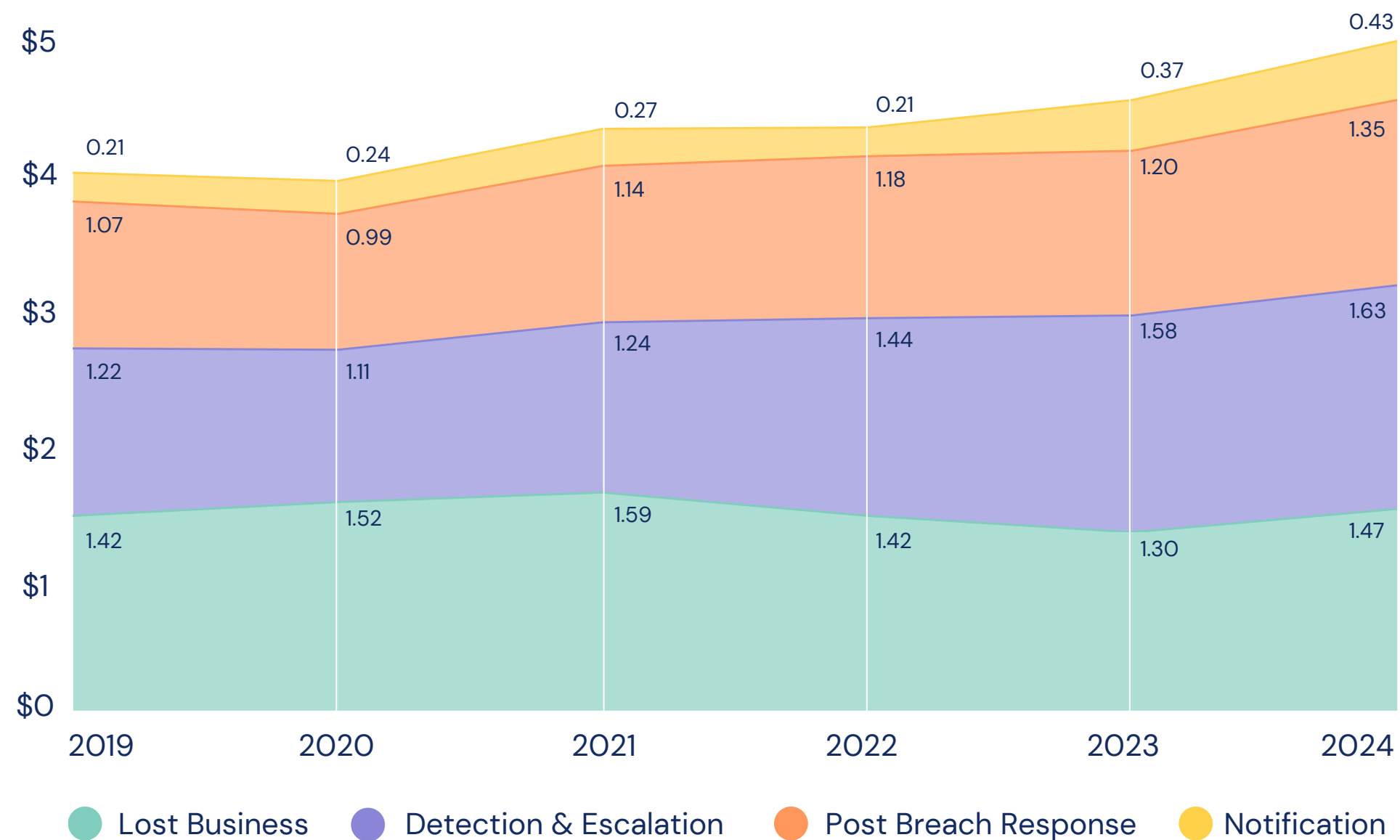


Walmart, Google, Microsoft, etc.

- **Cybercriminals steal** because it's easy to see quick results.
- They're not looking for the biggest fish to catch, they're **looking for the easiest**
- An estimated **15–30% of Americans are scammed in a year, losing \$1,600 on average**
- Higher rate of individuals being scammed among **lower-income adults with less education**

2 Cybersecurity is less expensive than a breach

Average cost of a data breach measured in millions of USD



Cyber attacks on small businesses can cost **thousands to millions of dollars** when you factor in the following:

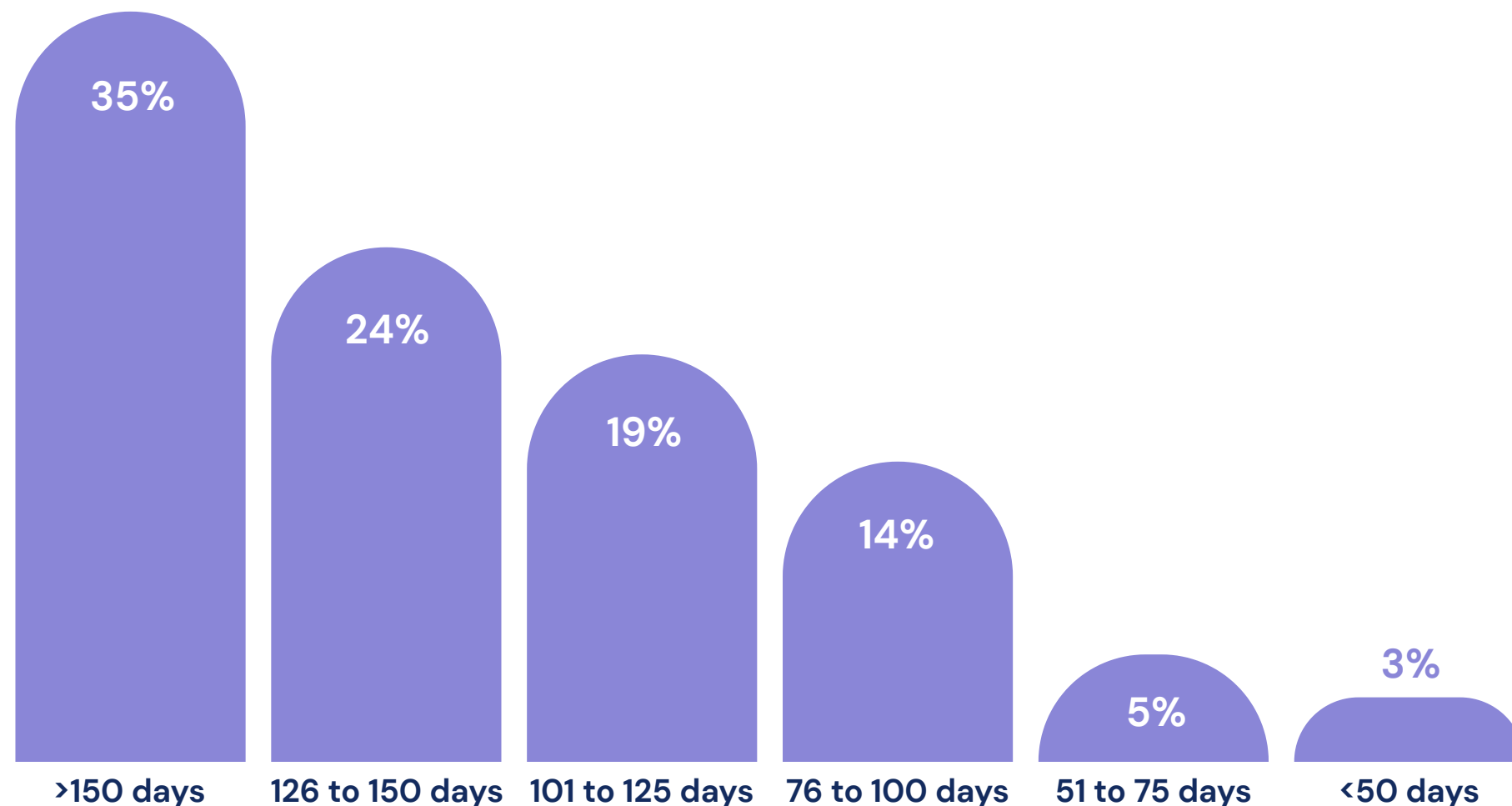
- Stolen money
- Downtime
- Disaster recovery resources
- Legal fees
- Repairing damaged reputation

Basic cybersecurity tools and processes can cost as little as a few thousand dollars per year.

[IBM: Cost of a Data Breach Report 2024](#)

3 If cybersecurity slows you down, you're doing it wrong

- A breach can cost you days, months, and even years of productivity
- IBM surveyed organizations that underwent a data breach. This was the average recovery time (not including those that hadn't yet recovered):



Top 3 reasons people bypass security measures:

- 1** Convenience
- 2** Save time
- 3** Meet an urgent deadline

How much time does it really take?

Multi-Factor Authentication
30 seconds/login x 5 logins = 2.5 min

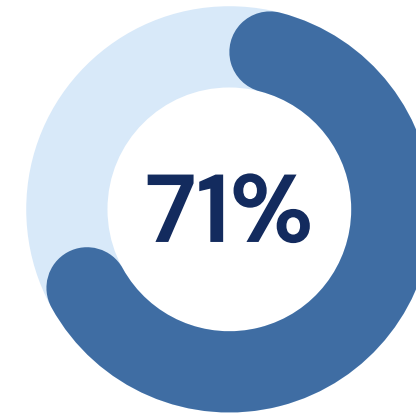
Software Updates
Automatic and can be done overnight

Security Awareness Training
5 min or less /month = 1 hour/year

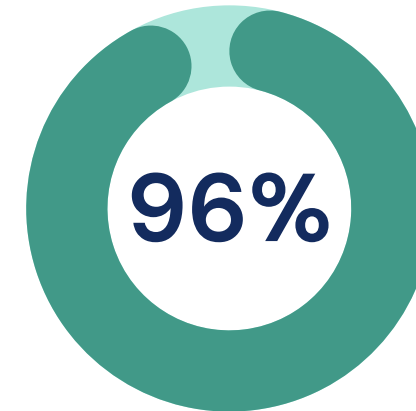
Review emails for phishing
7 seconds/email x 100 emails < 12 min

4 It's not about common sense – mistakes happen

- **Multitasking and working quickly** is a recipe for disaster
- People know cybersecurity basics but don't **make it a habit**
- Employees need **frequent reminders of why** cybersecurity is necessary and relevant to *them*

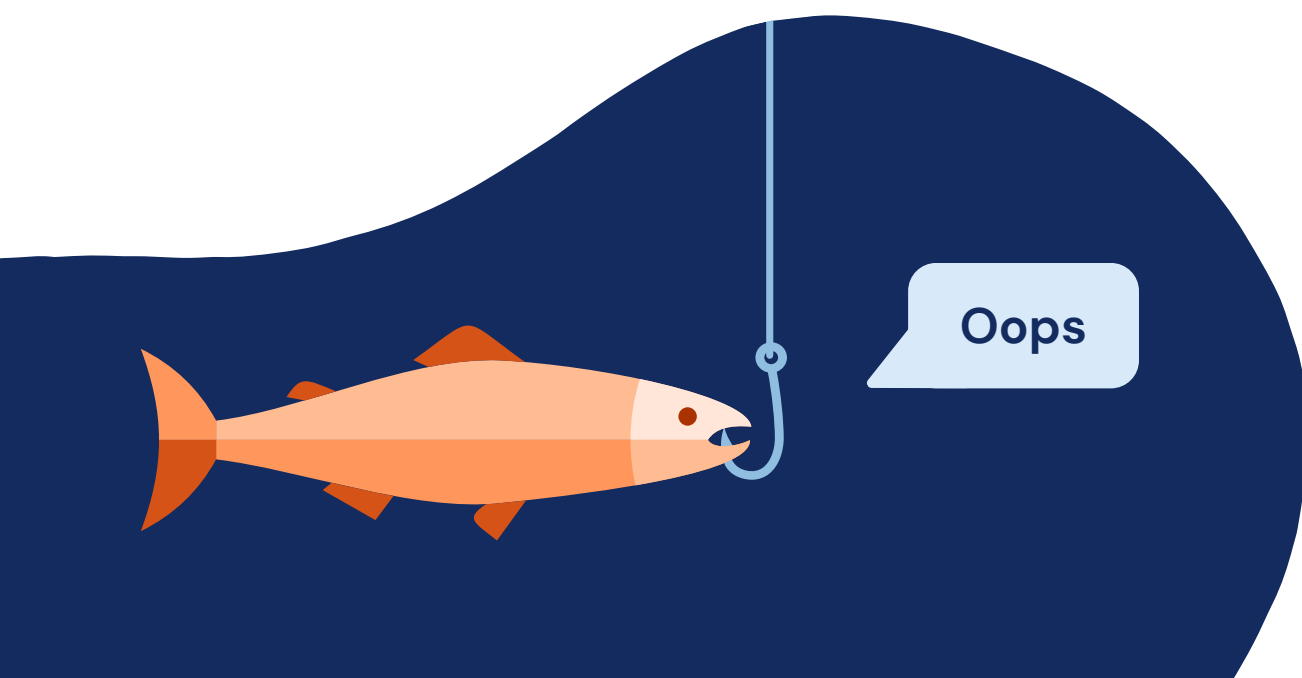


of surveyed users said they took a risky action in 2024



of users knew they were taking a risky action

Proofpoint: 2024 State of the Phish



Plus, technology changes so rapidly, and scams evolve with that technology. Employees need to be up to date on the most recent threats.

5 Once a year security awareness training is too long, boring, and irrelevant




Duration: <5 minutes

Frequency: 1 / month

Content: Engaging cartoon about a recent, real world cyber attack.

- Digestible
- Relevant
- Engaging



Everything you need to know to stay safe online

Duration: 1 hour

Frequency: 1 / year

Content: An overview of everything you need to know about cybersecurity.

- Overwhelming
- Irrelevant
- Boring

- Threats evolve constantly
- **Once a year training leaves you vulnerable** to new threats throughout the year
- **Annual** training tends to be **long and boring** (It's like studying for your 6th-grade history test, only to immediately forget everything once you go on summer vacation.)
- **Frequent and shorter trainings are easier to remember, more relevant, and more engaging**

Both = the same amount of training in 1 year

Why should you invest in
effective security
awareness training?

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

Employees at **small businesses are more likely to receive social engineering** attacks than employees at large enterprises.

Top 3 users most at risk of a breach



Users with access to business-critical data



Click happy users



Users who consistently fail to complete training



Phishing is the...

2nd
most prevalent
attack method

3rd
most costly
attack method *(avg of \$4.88M)*

[IBM: Cost of a Data Breach Report 2024](#)

- It can take **over 250 days to respond to phishing** and social engineering attacks
- SAT is proven to **reduce phishing clicks**

What's holding
you back?