PHIN

Top 5 Cybersecurity Excuses Hurting Your Business

My business is too small to be targeted in a cyberattack ✗

An estimated 15-30% of Americans are scammed in a year, losing $1,600 on average

0% 15% 30%
IPX 1031

Most cybercriminals are looking for the **easiest fish to catch**, not the biggest.

↓ Income ↑ High scam rate
Gallup
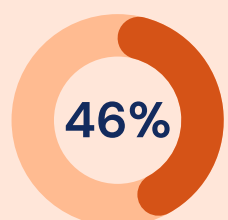
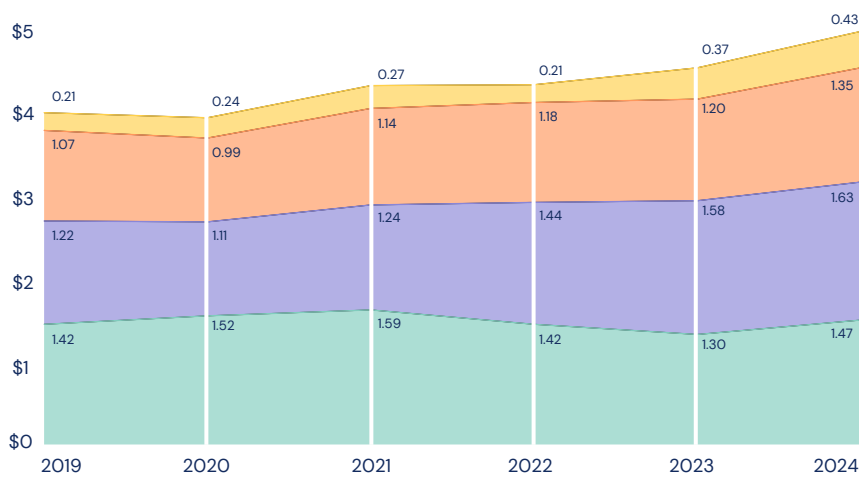**46%** of all cyber breaches impact businesses with less than 1,000 people
SecureWorld

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?

Average cost of a data breach measured in millions of USD

	2019	2020	2021	2022	2023	2024
Notification	0.21	0.24	0.27	0.21	0.37	0.43
Post Breach Response	1.07	0.99	1.14	1.10	1.20	1.35
Detection & Escalation	1.22	1.11	1.24	1.44	1.58	1.63
Lost Business	1.42	1.52	1.59	1.42	1.30	1.47

● Lost Business ● Detection & Escalation ● Post Breach Response ● Notification

IBM: Cost of a Data Breach Report 2024

Cybersecurity is too expensive ✗

You'll **spend more on a breach** than on cybersecurity.

Cost of a breach includes:
- Stolen money
- Legal fees
- Downtime
- Disaster recovery resources
- Repairing reputation

Embroker

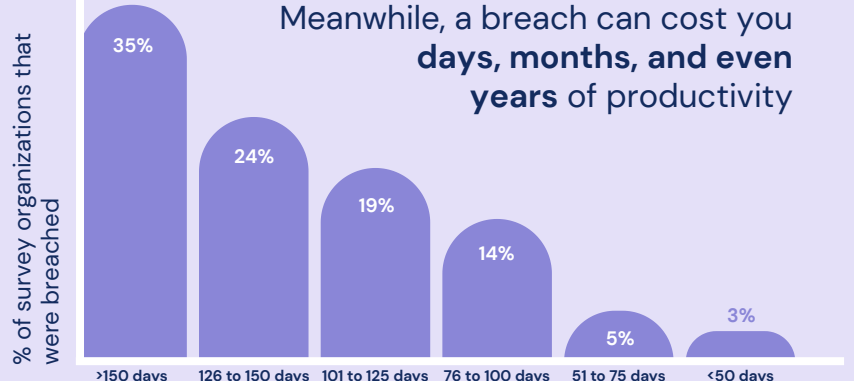**Cybersecurity is a productivity blocker** ✗

🕐 How much time does it really take?

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

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

Software Updates
Automatic and can be done overnight

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

Top 3 reasons people bypass cybersecurity:
Proofpoint: 2024 State of the Phish

1. Convenience
2. Save time
3. Meet an urgent deadline

Meanwhile, a breach can cost you **days, months, and even years** of productivity

% of survey organizations that were breached

>150 days	126 to 150 days	101 to 125 days	76 to 100 days	51 to 75 days	<50 days
35%	24%	19%	14%	5%	3%

Recovery time of surveyed organizations that experienced a breach
IBM: Cost of a Data Breach Report 2024

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

Proofpoint: 2024 State of the Phish

Human error is the #1 cause of breaches.

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

IBM: Cost of a Data Breach Report 2024

SAT is proven to **reduce phishing clicks**

Cybersecurity is common sense and doesn't require training ✗

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

96% of users knew they were taking a risky action
Proofpoint: 2024 State of the Phish

It can take **over 250 days to respond to phishing** and social engineering attacks

2nd most prevalent attack method

Phishing is the...
IBM: Cost of a Data Breach Report 2024

3rd most costly attack method

Once a year security awareness training (SAT) is enough ✗

It's like studying for your 6th-grade history test, only to **immediately forget everything** once you go on summer vacation.

✓

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

Both = the same amount of training in 1 year

Start training your users, today!

Sign up for free

PHIN