

Why Invest in Security Awareness Training?

Statistically Speaking

Whether you think cybersecurity is too expensive, your business is too small to be targeted in a cyber attack, or your employees don't need lessons on common sense — **we have news for you.**

Security awareness training (SAT) is worth every penny when done right.

This eguide will walk you through the most common excuses for neglecting cybersecurity and how that can impact your business, especially when it comes to SAT.

WHAT TO EXPECT

01

Top excuses for not investing cybersecurity

02

The truth behind these excuses

03

Why invest in SAT?



Top Excuses for Not Investing in Cybersecurity

My business is
too small to be
targeted in a
cyberattack



Cybersecurity is
a productivity
blocker



Once a year
security
awareness training
is enough



Cybersecurity
is too expensive



Cybersecurity
is common sense
and doesn't
require training



These **excuses** are hurting your business.

You might think avoiding cybersecurity is saving you money, but it's actually doing more harm than good.

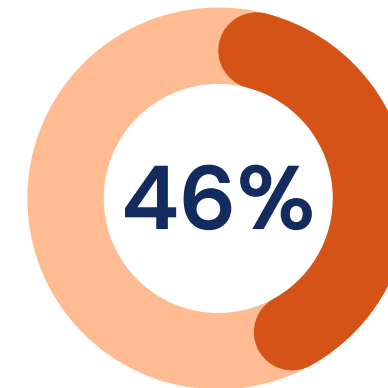
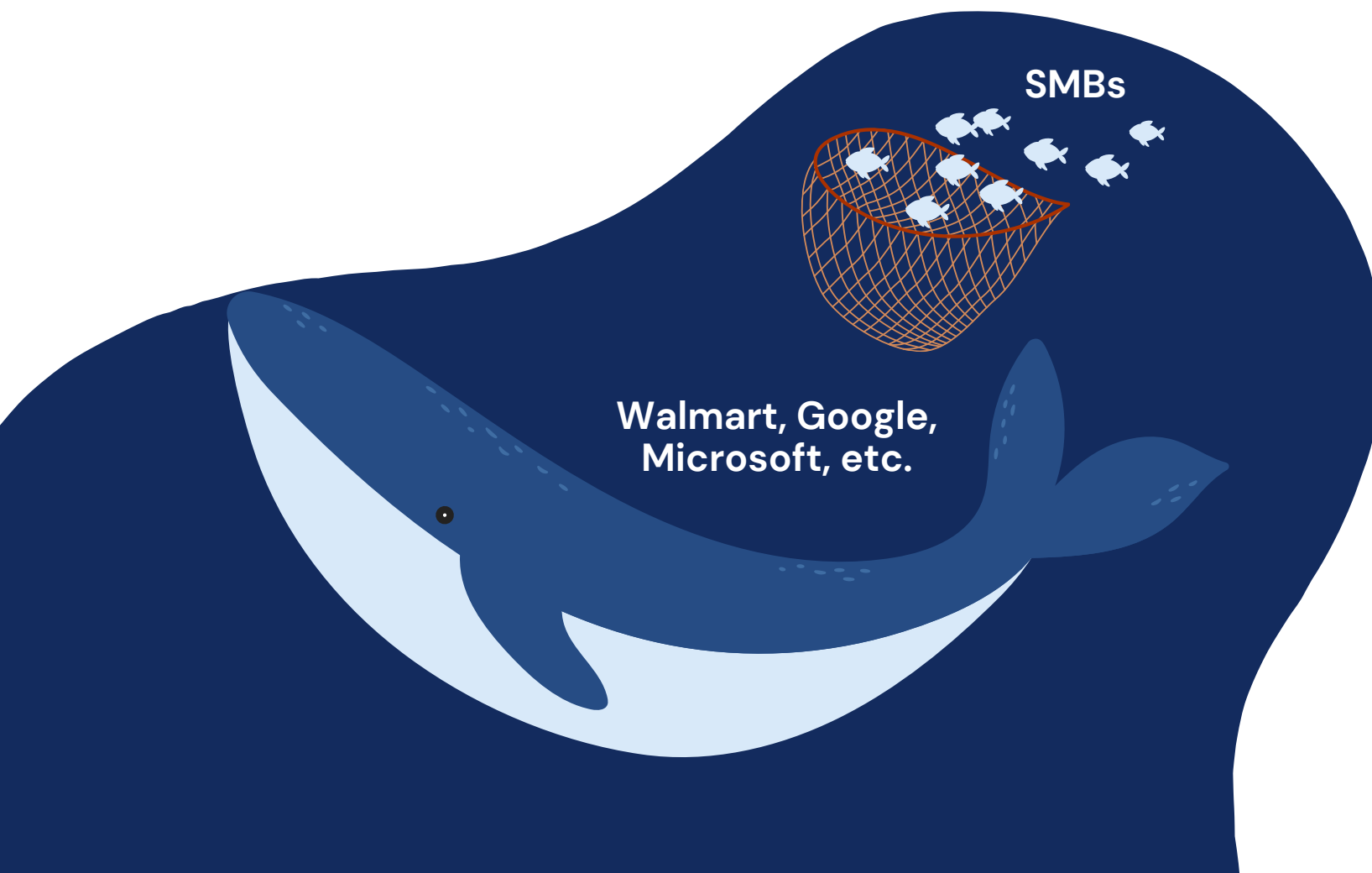
Here's why



1 No business is too small for a cyberattack

Why do cybercriminals steal? It's easy to see **quick results.**

They're not looking for the biggest fish to catch; they're looking for the easiest fish to catch. It takes less resources to catch 100 vulnerable little fish in a big net than it takes to catch a big blue whale who will undoubtedly tip your boat over.



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

[SecureWorld](#)

An estimated 15–30% of Americans are scammed in a year, losing \$1,600 on average, and the rate of individuals being scammed is higher for lower-income adults with less education.

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?**

2 Cybersecurity is less expensive than a breach

Start with the basics. This includes things like security awareness training, a password manager, data backups, cyber insurance, and an incident response plan.

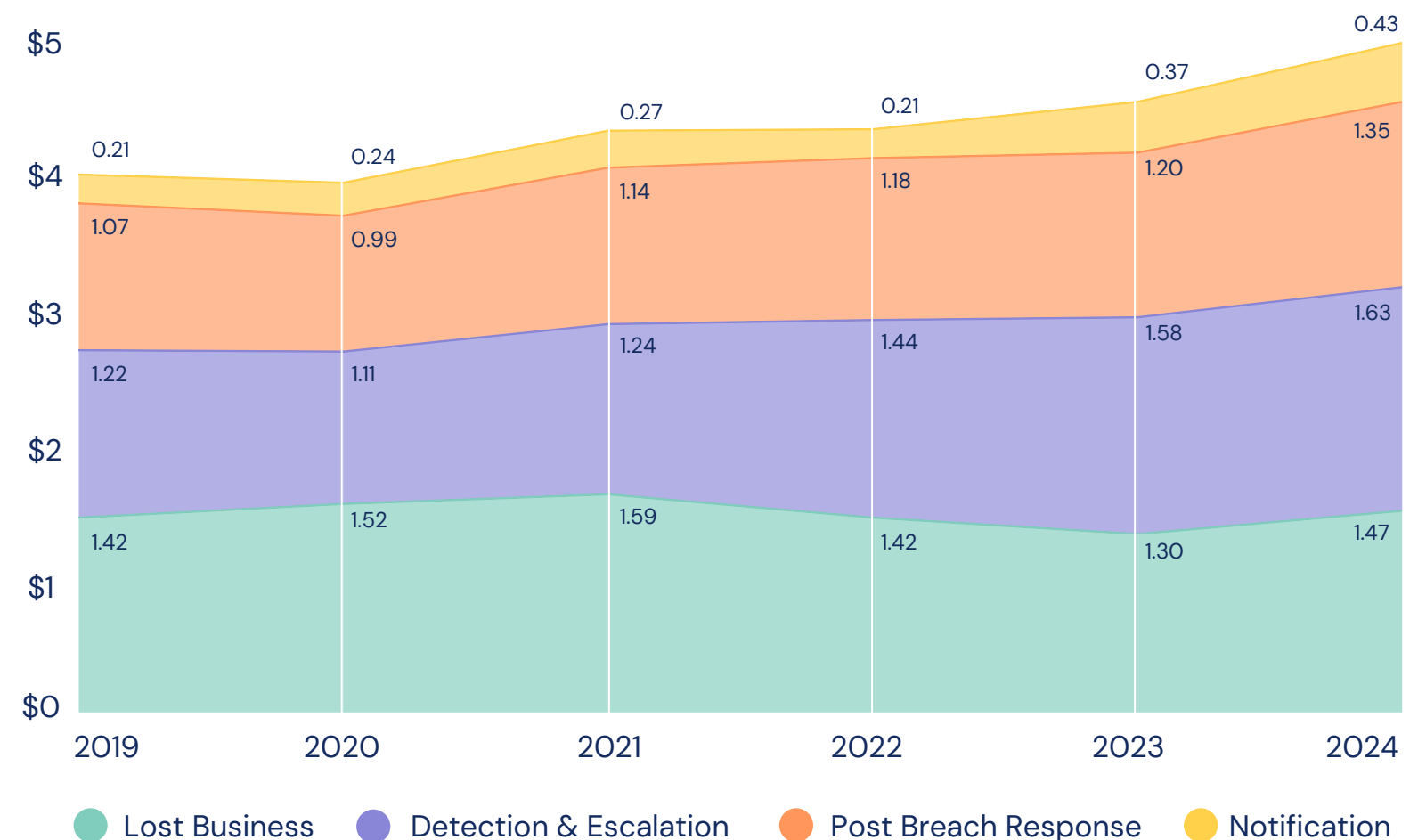
Cyber attacks on small businesses can cost thousands to millions of dollars when you factor in the following:

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

Meanwhile, implementing **basic cybersecurity tools and processes could cost as little as a few thousand dollars a year**, and they'll protect your data, money, reputation, and customer relationships.

With all of the different tools out there, **cybersecurity can seem expensive and daunting. But it shouldn't be all or nothing.**

Average cost of a data breach measured in millions of USD



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

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

Good cybersecurity won't slow you down. It might actually save you time.

Most people bypass security measures for convenience or to save time, but without cybersecurity in place, it's **not a matter of if, but when you'll get breached**.

A breach can cost you days, months, and even years of productivity. Meanwhile, "inconvenient" cybersecurity practices generally only add a few seconds or minutes to your day.

If your tools and processes are impacting your employees so much that it's reducing productivity, it **might be time to reevaluate the systems** you have in place.



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

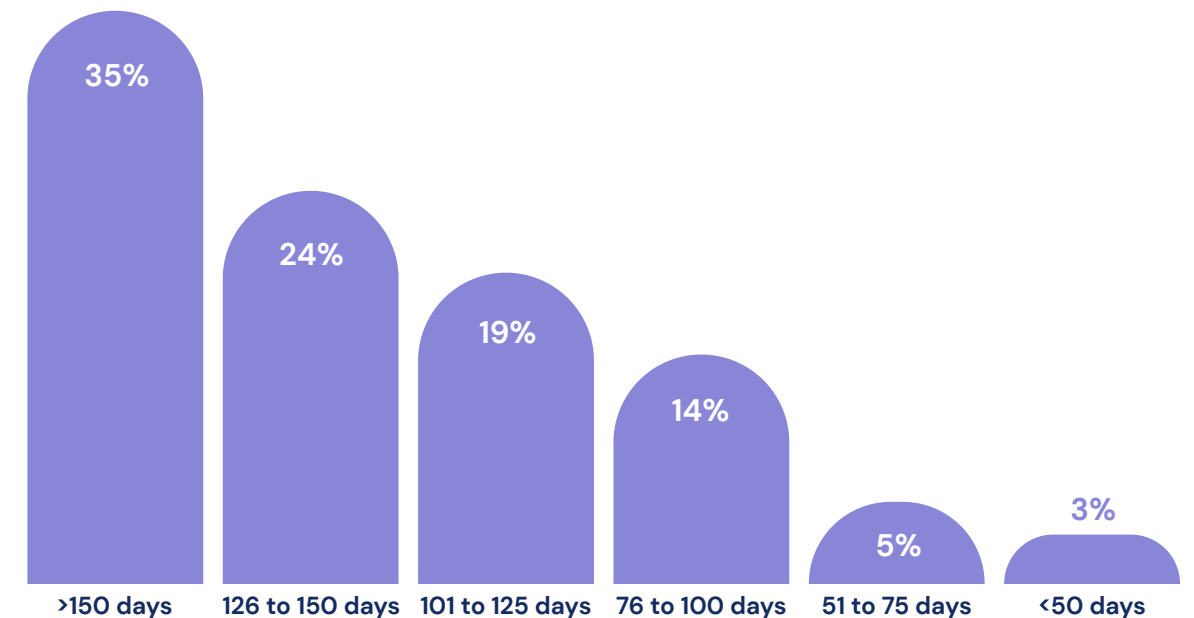
Software Updates

Automatic and can be done overnight

Review emails for phishing

7 seconds/email x 100 emails < 12 min

In 2024, IBM surveyed organizations that had undergone a data breach. Of the organizations that reported they had recovered from a data breach, this was their average recovery time, with **just 3% of businesses recovering in 50 days or less**:



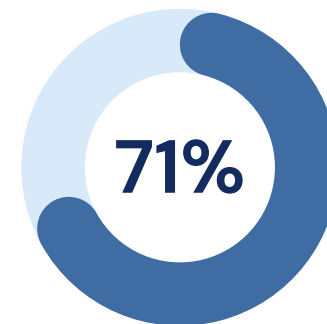
That's a lot of time and resources spent on **recovery** that could otherwise be spent growing your business.

4 It's not about common sense – mistakes happen

Employees are often **multitasking or working quickly** – especially at small businesses. This is the **perfect environment for an accident**.

Most **people know basic cybersecurity practices**, but they **don't make them a habit**. This leads to bypassing cybersecurity measures both accidentally and purposefully.

Why don't they make it a habit? They're don't understand **why cybersecurity is relevant to them**.

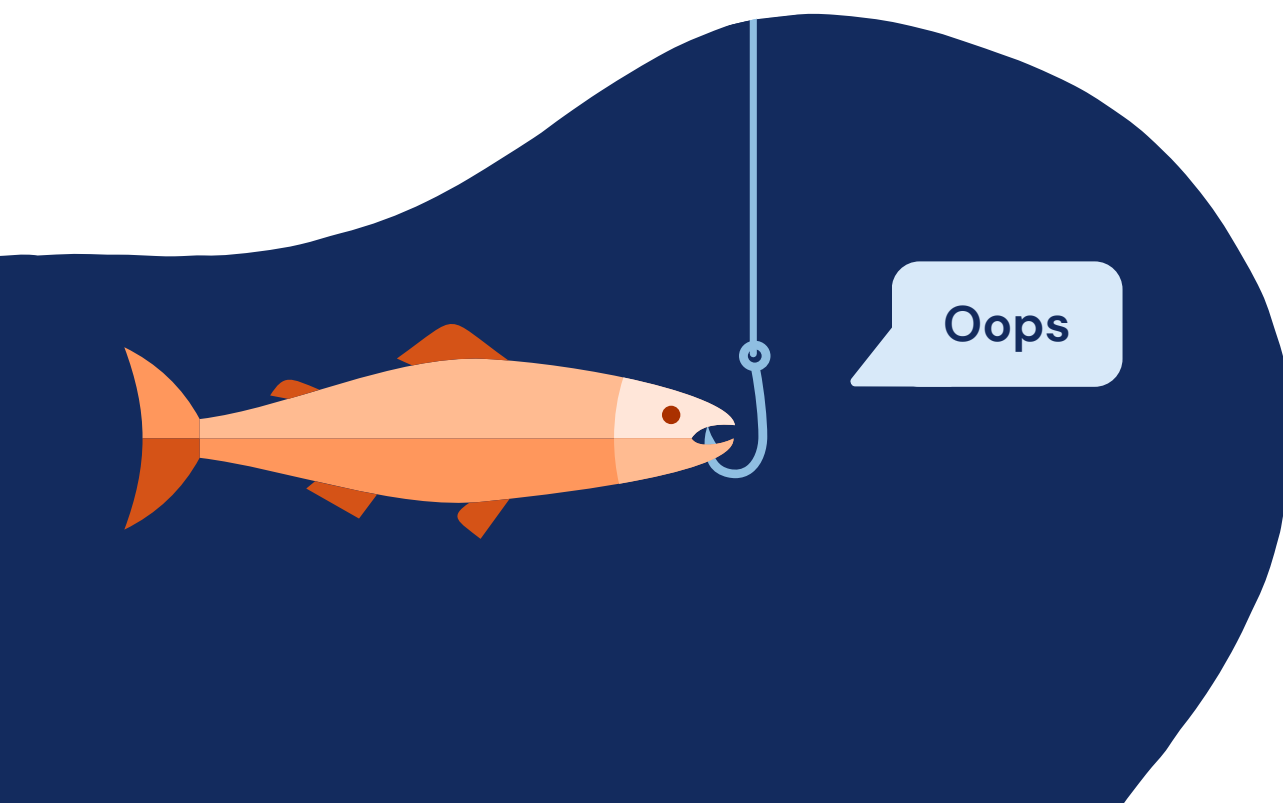


of surveyed users said they took a risky action in 2024



of users knew they were taking a risky action

[Proofpoint: 2024 State of the Phish](#)



Additionally, not everything is common sense. **Technology changes so rapidly, and scams evolve with that technology.** We're constantly experiencing new threats and tactics we've never seen before, so up-to-date and relevant training is 100% necessary.

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

Frequent and shorter trainings are easier to remember, more likely to hold your attention, and the content will be more relevant to current threats and trends.



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. If you're only **training once a year**, you're leaving your business wide open to a **plethora of threats that develop between annual trainings**.

Plus, it's highly **unlikely you'll remember information from annual training**. It's like studying for your 6th-grade history test, only to immediately forget everything once you go on summer vacation.

Once-a-year training tends to be much longer than more frequent training. This means **people get bored** and just play the training in the background of whatever they're working on, **so they're not retaining any information**.

Why should you invest in
effective security
awareness training?

Human error is the #1 cause of breaches.

You should invest in SAT that is **frequent, digestible, and relevant** to your employees.

Security awareness training shouldn't just check a compliance box. When done well, it's proven to change behavior. Users who consistently don't complete their training are in the top 3 most at risk groups of a cyber breach.

SAT is proven to reduce phishing clicks, which is crucial considering the average cost and frequency of phishing attacks exceeds most other cyber threats.


Phishing as an attack method


2nd
most prevalent

3rd
most costly
(at an avg of \$4.88M)

IBM: Cost of a Data Breach Report 2024

Top 3 most at risk users

 Users with access to business-critical data

 Click happy users

 Users who consistently fail to complete training

It can take over 250 days to respond to phishing and social engineering attacks, both of which are less likely to occur if you've deployed good SAT.

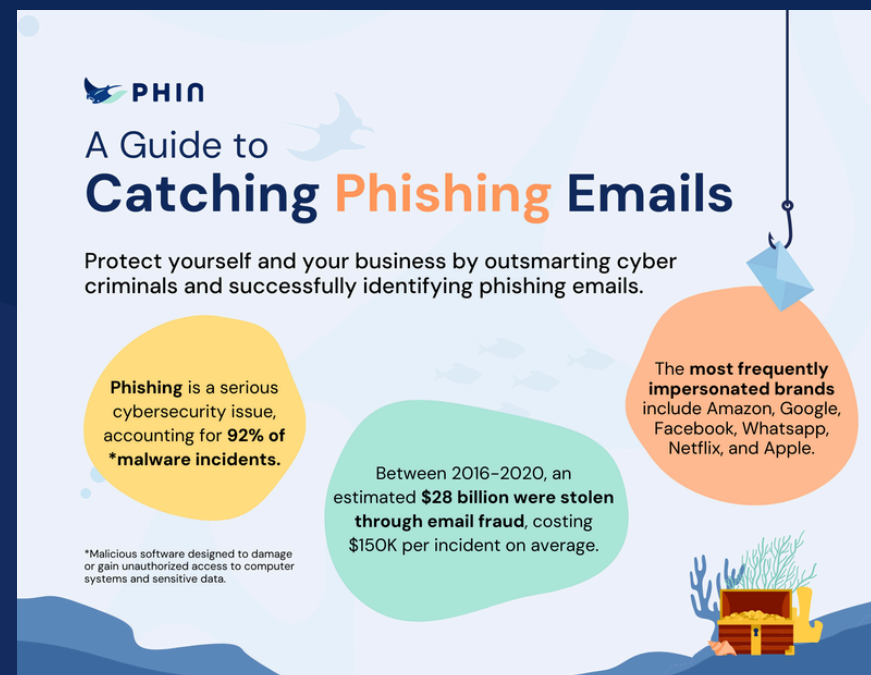
Employees at small businesses are more likely to receive social engineering attacks than employees at large enterprises, likely due to their lack of resources. So, it's especially crucial that small businesses give their employees the tools and information they need to identify and report cyber threats.

Deploying effective **security awareness training** is just **common sense**, especially for small businesses that are particularly at risk of social engineering attacks.

You should **never underestimate** the role **your employees** play in preventing a breach.

Ready to implement training?

START A FREE TRIAL, TODAY!



Don't wait until you have training in place to educate your users.

DOWNLOAD EGUIDES