for MSP Sales Teams

This is an internal reference to be used by Phin partner sales teams to facilitate conversations with their clients. This document contains confidential information and may not be shared externally.

The problem to lead with

Most cyber attacks involve a human mistake, with 46% of all cyber breaches impacting businesses with less than 1,000 people. Even if your clients already have a security awareness training (SAT) and phishing simulation platform, many tools miss the mark. They're cumbersome to manage, costing hundreds of hours in hidden labor, they suck you into long-term contracts, and they provide boring, irrelevant training content that users tune out.

Your clients need 3 things out of security awareness training (SAT):

1. A tool that can **prove ROI** and that keeps their MSP (you) **focused on high value activities**.
2. **Accurate, relevant training** that keeps their employees focused on high value activities.
3. Training that doesn't just meet compliance requirements but **improves end-user behavior**.

Why clients love Phin

Feature	Client Benefit
Report phishing button & instant feedback on phishing clicks	Instead of punishing end-users, mistakes are turned into *Learning Moments* to facilitate changes in user behavior.
Short, engaging content (75% under 5 minutes)	Content is more digestible and frequent, without disrupting the end-users' day-to-day responsibilities.
No login required	Access training directly via email — zero friction.
AI supported email analysis	Faster time to reported email resolution gives quicker insight into active cyber threats.
Insightful Reporting	Executive summaries, "users to watch", & long-term trend data shows ROI.

Why MSPs win with Phin

Feature	MSP Benefit
10-minute onboarding	Add new tenants instantly — no pre-purchasing.
Automated campaigns	Set-it-and-forget-it training and phishing campaigns that run themselves after initial 10-minute setup.
Self-service billing	Add/remove users instantly with Azure or Google sync. No new tickets or contracts required.
Multi-tenant dashboard	Manage all clients individually or in bulk from one dashboard.
Automated training reminders	Stop chasing end-users, Phin does it for you.
Integrations	Open APIs, Microsoft & Google integrations, and PSA integrations reduce manual labor and keep information all in one place.
Automated allowlisting and user syncs	You don't have to worry about phishing simulations not hitting your users inbox or your all of your users not getting trained. Phin's got you,
AI powered reported email analysis	Reduce escalations and increase time to resolution with URLs, headers, and AI severity shown right in your help desk.
White label branding	Deliver training as your own managed offering.
Internal NFR License	Use Phin internally for free.

Proof that Phin works

94% reduction
in time spent on SAT
(CCB Technology)

View Case Study

15 min → 3 min
time to resolution reduced per email with Phin AI triaging *(Certified CIO)*

View Case Study

1,100 new users
onboarded in 24 hours
(Fortify Technology)

View Case Study

25 hours
of labor saved per week on email triaging
(Velocity Networks)

"Phin speeds up time to value for our clients."
– CCB Technology

"You've reduced the human error rate... not just on the end user side, but also on the engineer side."
– Certified CIO

"Easiest deployment of any platform I've worked with."
– Fortify Technology

How to position Phin to clients

Phin gives your end-users the awareness to stop threats before they start without adding tedious work to their IT teams (aka you).

"We already do security awareness training once a year. We don't want to distract our employees."

→ Most of Phin's content takes 5 minutes or less. Delivered monthly, that equals 1 hour for the entire year, but is more digestible and engaging than annual training.

"We can't manage another tool."

→ Phin runs itself — you just need to review reporting.

"It's too expensive."

→ Phin has extremely competitive pricing and its automation reduces labor costs.

Other providers

- KnowBe4
- Breach Secure Now
- Curricula
- Bullphish
- Ironscales
- Proofpoint
- And more

How Phin Wins

- Real time feedback on phishing simulations
- Content is frequently updated and sourced from 7 different providers
- Automated reporting to track user behavior changes
- AI powered email triaging built right into the MSP's help desk
- No long-term contracts
- Billing based on actual usage month-to-month
- Responsive support
- Less hidden labor
- SAT isn't an add-on, it's Phin's main focus

Phin's Impact

"After switching to Phin from KnowBe4, we have gotten much better feedback from customers, they enjoy the content, and engage more with it. Phin keeps the content much shorter, which is better for the end-user. " — Rake Digital

"Phin's trainings have a direct and immediate impact on reducing liability." — Simplex IT

"Our customers love Phin and have gotten better at catching and identifying phishing attempts." — Alleron IT

"Clients are really enjoying Phin; they find the training fun and engaging." — ITRA consulting

"Phin is a breath of fresh air in comparison to Bullphish. Our end users prefer the content and find the interface much easier and simpler to use." — Avtek Solutions

Phin is more than just security awareness training

1

AI Email Triaging

Phin extracts information from reported emails with the help of AI, such as headers, URLs, the email preview, severity and tags, which help you understand what kind of potential attack it might be. You can view all of this without leaving your help desk. Phin also lets you search for emails, delete emails, and block attackers all at once with a single button.

Why do your clients care?

This allows you to address and stop attacks more quickly, reducing the potential of a breach.

Key Benefits

- **Respond to malicious emails faster** — real threats no longer get lost among the spam
- **Stop threats before they even make it to the inbox** — If a malicious email is found in one tenant, it can easily be blocked across all other tenants
- **Reduce time wasted** — L1s can handle email triaging while higher level techs focus on larger threats

< 1 min Certified CIO's response time to reported emails with Phin.

2

Dark Web Monitoring

Run scans to check employee email addresses in a database of over 600 million compromised accounts from thousands of known breaches to see if their information is exposed.

Why do your clients care?

When a website or service gets hacked, stolen credentials often end up on the dark web where criminals buy and sell them. If employees reuse passwords between personal and work accounts and those passwords are exposed, your organization is at risk.

Key Benefits

- **Find compromised accounts fast** — Identify which employees have appeared in data breaches
- **Scan everyone at once** — Check your entire organization with one click
- **Know what's at risk** — See exactly what types of information were exposed
- **Scan anytime** — Run scans whenever you need them