

CYBERHOOT VS TRADITIONAL PHISHING

The best defense is a positive offense

Looking for better results from your security awareness training? Where traditional phishing tests use 'gotcha' tactics that trick employees into failure, CyberHoot's positive reinforcement approach trains them to recognize and report real threats.

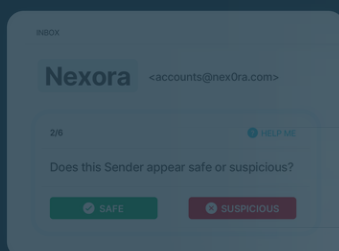
[Get Started](#)[Book a Demo](#)

Organizations choosing positive reinforcement

RedZone
TECHNOLOGIES

SINGLE DIGITS

cmIT Solutions
Your Technology Team



✓ This is a suspicious SENDER and you knew it!

THE PROBLEM

Your employees dislike traditional phishing tests

✗ They trick

Fake phishing emails are designed to catch employees out, increasing stress without improving results.

✗ They punish

Traditional testing punishes those who make mistakes, forcing additional training that lowers morale.

✗ They fail

Typical simulation training is unengaging, so users drop off and fail to learn the security awareness they need.

[Get Started](#)
[Book a Demo](#)

THE CYBERHOOT DIFFERENCE

Stop attacking. Start supporting.

The research is clear. Fake phishing tests and “fail” grades don’t encourage employees and can actually increase vulnerabilities by making employees more anxious, less confident, and more likely to click. CyberHoot’s positive reinforcement builds genuine security awareness.

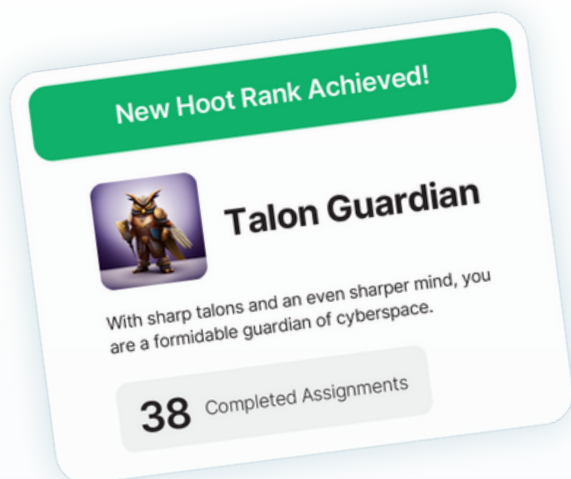
POSITIVE REINFORCEMENT

Don’t create anxiety. Build confidence.

Fake phishing emails designed to catch employees out create stress and reduce trust between employees and IT teams.

CyberHoots interactive training teaches employees how to spot threats, building genuine security awareness through positive reinforcement.





INCREASED SECURITY

Address real threats with realistic scenarios

Attack phishing simulations use simple, predictable domains that don't match the vendors they impersonate, making them easy to spot and failing to build real awareness.

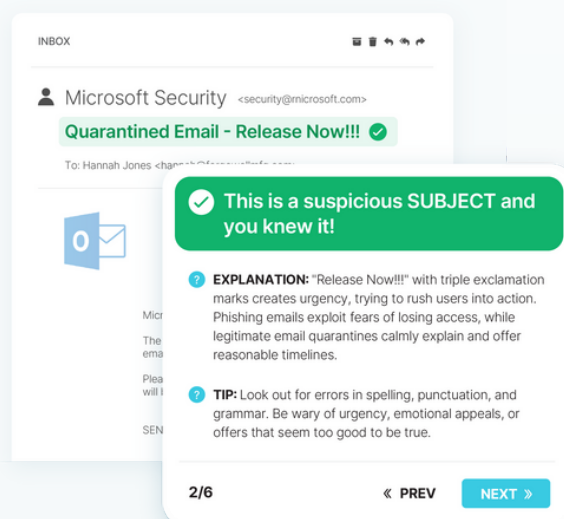
CyberHoot uses hyper-realistic scenarios that teach employees to recognize actual threat indicators via interactive walkthroughs.

INCREASED ENGAGEMENT

Positive gamification beats negative training

Traditional static training models are dull and unengaging. Black Hat research found over 50% of employees abandon them in under 10 seconds, leaving gaps in your security awareness.

CyberHoot's interactive, gamified approach keeps employees engaged and builds lasting behavior change.

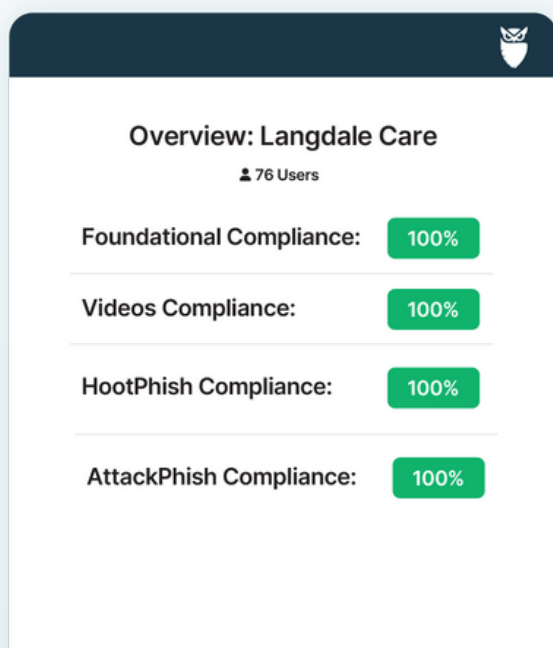


SMARTER ANALYTICS

Complete visibility drives measurable improvements

Traditional phishing emails are often only tracked when a user clicks. If employees ignore the email, you get zero insights into their security readiness.

CyberHoot's interactive training monitors every individual user's progress with 100% visibility for all users, tracking improvements, and identifying weak links.



CYBERHOOT VS TRADITIONAL VENDORS

Expanding protection across the educational community

CyberHoot

Other Vendors

APPROACH

Learning Method

✓ Positive reinforcement

✗ Negative "gotcha" testing

Training Type

✓ Interactive + realistic

✗ Traditional phishing emails

Simulation

✓ Hyper-realistic

✗ Over-simplified

CyberHoot

Other Vendors

EFFECTIVENESS

Engagement Rate

✓ High with gamification and rewards

✗ 50%+ abandon training in under 10 seconds

Completion Rate

✓ Near 100% & measurable

✗ Averages just 24%

Employees

✓ Build confidence and trust

✗ Feel tricked and anxious leading to disengagement

Improvements

✓ 19% better results with a positive approach¹

✗ Just 1.7% overall improvement

Behavior Change

✓ Long-term

✗ Minimal change

CyberHoot

Other Vendors

FEATURES

Interactivity

 Fully gamified

 Static, limited

Analytics

 Individual user reports

 Limited

Customization

 Tailored + White-Label

 Limited

Video Training

 1,000+ videos on security topics

 Available

Automation

 Full - training, emails, reminders, reports

 Partial

Setup Complexity

 Simple, deployed in minutes

 Moderate to high complexity

Integration

 Effortless with Microsoft 365 and Google Workspace

 Varies by vendor

Dark Web Monitoring

 Yes

 Not typically

MSP Multi-Tenancy

 Yes

 Partial and difficult

THE WISE CHOICE

Swap outdated attack phishing simulations for:



Positive reinforcement

that builds confidence,
not anxiety



Automated training

that works without
constant management



Interactive engagement

that employees
actually enjoy



Proven results

that reduce real-world
phishing success

TESTIMONIALS

What our customers say...

Exceptional Value: *"Using CyberHoot was one of the best decisions we made regarding SAT. Fully automated, training is interesting, and staff participation is high compared to other vendors."*



Michael Gibby, SEQ IT Services, Founder & Managing Director

Exceptional Results: *"After 9 months of CyberHoot awareness training, a Financial Management firm with \$4 Billion in assets was phish tested by the Fellsway Group. They had zero (0%) employees click on the phishing test. In contrast, the exact same phishing attack had a 30% click rate at another client that had not yet done CyberHoot training. The product really proves its worth!"*



John Mumford, Chief Risk Officer at the Fellsway Group (A Consulting Firm)

Exceptionally Easy: *"CyberHoot is an excellent cybersecurity training platform that educates teams on security practices through training content, phishing simulations, and actionable analytics."*



Tim Ward, Goodwill of Chattanooga, Director, Information Technology

GET STARTED

Stop tricking employees. Start training them.

Join the leading organizations choosing positive reinforcement
over punishment for security awareness training.

Get Started

Book a Demo

www.cyberhoot.com

SOURCES

The Impartial Research

Check out the sources below or review the detailed white paper.

- Mirian, A., Dameff, C., Ho, G., et al. (2024). "Understanding the Efficacy of Phishing Training in Practice." Presented at Black Hat USA 2024. University of Chicago & UC San Diego Health.
- Schöps, M., et al. (2024). "The Impact of Security Awareness Training on Employees' Self-Efficacy." USENIX Security Symposium.
- Wash, R., & Cooper, M. (2018). "Who Provides Phishing Training? Facts, Stories, and People Like Me."
- <https://arxiv.org/pdf/2112.07498.pdf> **Phishing in Organizations: Findings from a Large-Scale and Long-Term Study** Authors: Daniele Lain, Kari Kostiainen, and Srdjan Capkun ~ Department of Computer Science ETH Zurich, Switzerland {daniele.lain, kari.kostiainen, srdjan.capkun} @inf.ethz.ch