Case Study:

Positive reinforcement. Automated efficiency. Cybersecurity training that transforms.

Goodwill Industries of the Greater Chattanooga Area + CyberHoot

The Client

Goodwill Industries of the Greater Chattanooga Area

Tim Ward
Director, Information Technology

Founded in 1935, Goodwill Industries of the Greater Chattanooga Area serves 23 counties across Southeast Tennessee and Northwest Georgia. As an affiliate of Goodwill Industries International, their mission is clear: transform lives and communities through the power of work.

Operating retail stores, workforce development programs, and community services, Goodwill helps individuals achieve personal and professional goals while diverting millions of pounds of waste from local landfills. Their Opportunity Campus and Opportunities Center provide education, training, and job placement services to remove barriers to personal success.

With a diverse workforce spanning retail operations, mission integration specialists, and IT professionals, protecting sensitive data and maintaining cybersecurity compliance is essential to their community-focused mission.

The Challenge

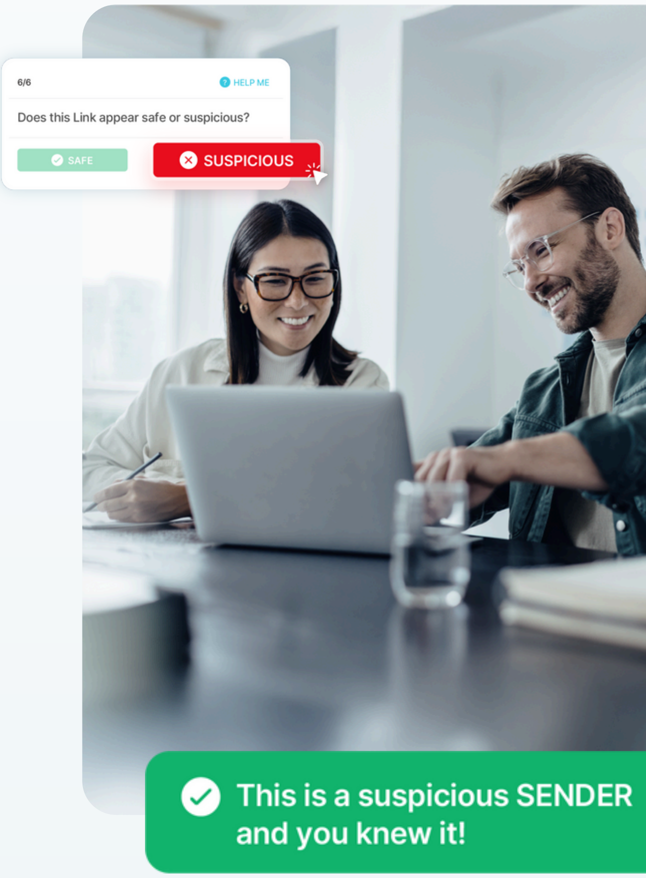
Manual processes and punitive approaches undermining security culture

"The previous methods focused more on punitive measures for bad behaviors, such as clicking on phishing links, rather than positive reinforcement. This approach sometimes led to negative employee engagement and resentment towards the IT department."

Before CyberHoot, Goodwill's cybersecurity training approach created more problems than it solved. Their manual system required significant effort to set up, administer, and troubleshoot phishing simulations and training programs, often leading to delays and inefficiencies.

The organization faced several critical challenges:

- **Punitive training approach:** Traditional methods focused on catching employees making mistakes rather than teaching them to avoid threats
- **Manual administration:** Time-intensive setup and management of phishing simulations and training
- **Low engagement:** Negative reinforcement created resentment toward the IT department
- **Compliance gaps:** Less automated tracking and reporting made oversight difficult
- **Unrealistic simulations:** Oversimplified phishing tests gave employees a false sense of security
- **Growing threat landscape:** Sophisticated nation-state attacks from countries like Russia and China demanded better preparation



Does this Link appear safe or suspicious?

This is a suspicious SENDER and you knew it!

The existing approach failed to build a positive relationship between employees and IT that's essential for an effective cybersecurity culture.

The Solution

Automated platform built on positive reinforcement, not punishment

> *"CyberHoot uses a positive reinforcement approach to teach cyber literacy skills. This method encourages good behaviors, builds knowledge, and teaches users how to recognize and avoid phishing attempts without punitive measures."*

Goodwill discovered CyberHoot through a colleague's recommendation during their evaluation of cybersecurity solutions. What immediately stood out was CyberHoot's fundamentally different philosophy: teach, don't trick.

Key differentiators that attracted Goodwill included:

Positive reinforcement approach:

Instead of punishing mistakes, CyberHoot's HootPhish training guides employees through realistic scenarios, teaching them to identify threats through interactive and engaging experiences.

Zero-setup automation:

The platform requires no daily management, eliminating the administrative burden that consumed IT resources.

Hyper-realistic simulations:

Unlike their previous oversimplified tests, CyberHoot uses typo-squatted domains and authentic hacker tactics to prepare employees for real-world threats.

Comprehensive reporting:

Granular insights identify individual weaknesses with actionable improvement advice.

The onboarding process proved remarkably straightforward. Goodwill simply imported a CSV file of users and managers, and CyberHoot handled the rest.

"It was a pleasure to have such simple onboarding steps."

CyberHoot's passwordless user experience meant only administrators needed to log in, while employees received training directly in their inboxes, eliminating password reset headaches.

The Results

Higher compliance, enhanced awareness, stronger security culture

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

The transformation was immediate and measurable. Goodwill's compliance reports showed consistently high completion rates across all cybersecurity training modules, including phishing awareness, password hygiene, and mobile device security.

Enhanced employee engagement: The positive reinforcement approach eliminated the adversarial relationship between employees and IT, creating genuine enthusiasm for cybersecurity learning

Improved cyber literacy: Employees developed lasting skills to recognize and avoid real-world phishing attacks, moving beyond simple compliance to genuine understanding.

Streamlined operations: Automation freed IT staff from manual training administration, allowing them to focus on strategic initiatives.

Actionable insights: Detailed reporting helped leadership understand specific vulnerabilities and track improvement across the organization.

Long-term value: Unlike previous short-term compliance training, CyberHoot equipped employees with a deep understanding of phishing tactics and threat recognition.

The internal feedback was overwhelmingly positive. Teams appreciated the engaging video content and quizzes delivered directly to their inboxes, finding the experience less stressful and more educational than previous approaches.

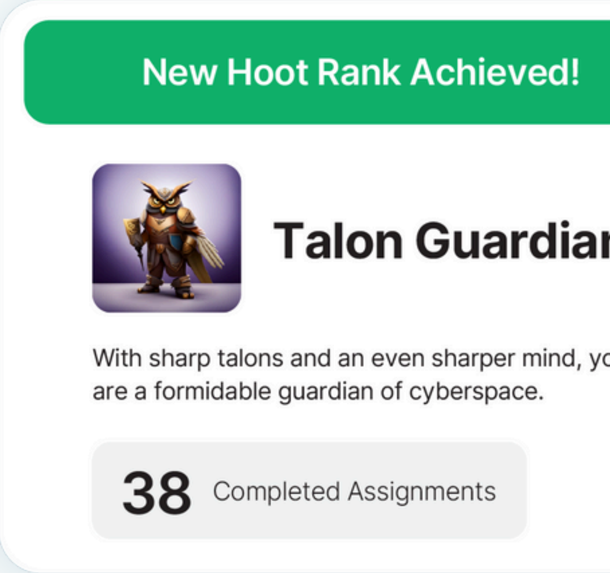
The Future

Future-proofing cybersecurity

> *"We'll certainly continue training our employees with CyberHoot, it is a wonderful tool in our Cybersecurity Arsenal."*

For Goodwill, CyberHoot has become integral to their long-term cybersecurity strategy. The platform's automated approach ensures consistent, engaging training that builds genuine security awareness rather than mere compliance.

As they continue their mission to transform lives through work, Goodwill can focus on serving their community, knowing their cybersecurity training runs seamlessly in the background, protecting both their organization and the people they serve.



New Hoot Rank Achieved!

Talon Guardiar

With sharp talons and an even sharper mind, yo
are a formidable guardian of cyberspace.

38 Completed Assignments

> *"CyberHoot's integration into our organization's long-term plans ensures a robust and proactive approach to cybersecurity, fostering a secure and knowledgeable workforce."*

Tim Ward
Director, Information Technology

CyberHoot

Summary

Challenge

- *Manual phishing simulations requiring extensive setup and troubleshooting*
- *Punitive approach creating employee resentment toward IT department*
- *Low engagement and compliance with traditional training methods*
- *Unrealistic simulations providing false sense of security*
- *Growing sophistication of nation-state cyber threats*

Solution

- *Fully automated cybersecurity training platform with zero setup requirements*
- *Positive reinforcement approach teaching through interactive HootPhish scenarios*
- *Hyper-realistic phishing simulations using authentic hacker tactics*
- *Passwordless user experience with inbox-delivered training*
- *Comprehensive reporting with granular insights and actionable advice*

Results

- *High compliance rates across all cybersecurity training modules*
- *Enhanced employee engagement and cyber literacy*
- *Elimination of IT department resentment through positive approach*
- *Streamlined operations with automated training delivery*
- *Long-term security awareness building beyond simple compliance*
- *Strong internal feedback and leadership support*

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

Tim Ward

Director, Information Technology

CyberHoot

Stop tricking employees. Start training them.

Get a grip of your security awareness training with the one-of-a-kind platform that uses fun, positive engagement to deliver more effective results.

Book a Demo

www.cyberhoot.com

Follow us for the latest news and updates