# Case **Studies**

In an era marked by ever-evolving cyber threats, organisations are realising the critical importance of equipping their workforce with the knowledge and skills necessary to defend against cybercrime.

These case studies delve into the realm of Security Awareness Training (SAT) within various industries, exploring how companies have successfully mitigated risk and fostered a cyber-savvy culture among their employees.

# Case Study

INDUSTRY - **FINANCE** LOCATION - **USA**

ORGANISATION SIZE - **70**

## Why It Mattered

Cyber attacks had left them uninsurable. With phishing incidents rising and no Security Awareness Training (SAT), they needed a way to meet IRS compliance and build a cyber-savvy workforce, without the bore of outdated seminars.

## The Problem

This accounting firm, managing sensitive financial data, was hit by a phishing attack and deemed uninsurable. Their MSP provided basic hourly training, but it didnt stick.
**They needed more than a checkbox exercise - they needed:**

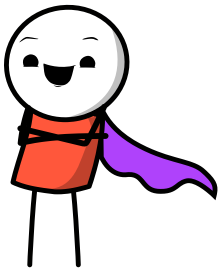
- A self-managed SAT platform
- Engaging, flexible content
- Simulated phishing drills
- Compliance with IRS standards

## The Solution: Goldphish

- Tailored monthly training
- Ongoing phishing simulations
- Seamless implementation
- Security culture transformation

## The Results

- No phishing attacks succeeded
- Reporting of phishing attempts surged
- Organisation regained insurability
- Security awareness became part of the culture



> “ We have not fallen victim to any subsequent phishing attempts since implementing Goldphish’s solution.

# Case **Study**

INDUSTRY - **INSURANCE** LOCATION - **USA**

ORGANISATION SIZE - **20+**

## Why It Mattered

When a major jewellery insurance firm initially approached Goldphish to meet audit requirements, they soon discovered that true cyber resiliance required an engaged workforce and consistent Security Awareness Training (SAT).

## The Problem

With over 2,500 clients nationwide, the company had two key challenges:

- Protecting organisational and client data
- Overcoming low employee engagement with existing SAT

They faced poor security posture, frequent phishing attacks, and ineligibility for cyber insurance - all exacerbated by audit failures.

## The Solution: Goldphish

How did we transform this organisation and create a cyber-savvy workforce?

- Seamless implementation
- Security culture transformation

> Goldphish has helped me make security awareness training readily and easily available to all employees.

# Case **Study**

INDUSTRY - **IT & SERVICES** LOCATION - **SA**

ORGANISATION SIZE - **30+**

## Why It Mattered

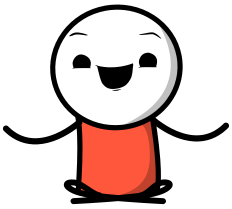
To strengthen cybersecurity and meet ISO27001 certification standards, they needed to elevate employee awareness. Handling sensitve data across industries, the stakes were high.

## The Problem

As a key consumer intelligence player, this company partners with over 80 major African banks, insurers, retailers, and healthcare providers.

Their challenges:

- Protect client and company data
- Manage remote work risks
- Meet ISO27001 certification
- Qualify for cyber insurance



Before Goldphish, employees had no formal SAT - making them a liability.

## The Solution: Goldphish

Goldphish delivered:

- Tailored SAT modules
- Simulated phishing campaigns
- A 12-month strategic security plan
- Regular assessments and progress reviews

This approach engaged employees with ongoing training, embedded security into daily routines, and boosted insurance eligibility.

## The Results

- Phishing attempt reporting jumped from 0% to 40%
- A culture of cybersecurity awareness took hold

> “ Goldphish has increased employees' cyber security awareness, and has resulted in an increase of 40% of reported phishing attempts.

# Case **Study**

INDUSTRY - **MARKETING & ADVERTISING**

LOCATION - **USA** ORGANISATION SIZE - **500+**

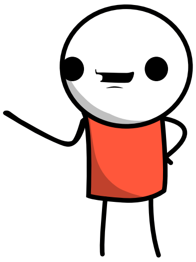
## Why It Mattered

A leading corporate communications agency's cybersecurity concerns left them uninsurable. Their lack of Security Awareness Training (SAT) and low employee engagement made them vulnerable - risky for clients and insurers alike.

## The Problem

Despite working with major global brands, this agency had no active SAT in place. Their previous efforts were minimal - a basic policy requiring employee acknowledgment, but no real training or phishing simulations. **They needed:**

- An effective SAT solution
- Tools to boost employee engagement
- Improved insurability
- A sustainable security culture



## The Solution: Goldphish

Goldphish was brought in by the client and their insurer to implement comprehensive SAT and phishing simulations. **Together they launched:**

- **Monthly bite-sized SAT training**
- **Simulated phishing campaigns**
- **Regular engagement with employees**
- **Progress tracking via executive reports**

> “ The shorter training campaigns have allowed the employees to complete training on a monthly basis and this has strengthened our overall cyber security posture.

## The Results *Following the rollout*

- **Employee engagement skyrocketed**
- **Phishing threat detection improved**
- **Insurability was restored**
- **Ongoing SAT became embedded in the culture**

Partnering with Goldphish, they strengthened their cyber defences and secured the trust of insurers and clients alike.