

ROYAL BANK OF SCOTLAND REDUCES PHISHING SUSCEPTIBILITY

SECURITY AWARENESS TRAINING CHANGES EMPLOYEE BEHAVIOR, REDUCES RISK



THE CHALLENGE

- Increase in malware entering RBS's system via email
- Lack of employee engagement in preventing phishing
- Risk of costly ransomware recovery

THE SOLUTION

- Proofpoint Anti-Phishing Training Suite
- Managed Services

THE RESULTS

- Lowered phishing susceptibility by more than 78%
- Improved engagement among stakeholders and employees
- Reduced successful cyber attacks

THE COMPANY

Established in 1727, the Royal Bank of Scotland (RBS) is a historic financial institution with a global presence. Headquartered in Edinburgh, RBS and its subsidiaries provide financial products and services for personal, commercial, corporate and institutional customers.

As RBS well knows, financial institutions are highly targeted by cyber criminals. The bank recognized that its 80,000 email users present a significant attack surface for criminals.

THE CHALLENGE

RBS was experiencing steady increases in phishing attacks and malware entering their system via email. Part of the problem was that many employees did not consider themselves responsible for detecting and avoiding phishing. RBS needed its staff to understand how their casual behavior with dangerous emails was causing real damage.

Lesley Marjoribanks, customer security manager and security awareness lead at RBS, volunteered to lead a security awareness training program. While RBS had briefly tried simulated phishing in the past, Marjoribanks knew she needed a more comprehensive program to engage employees and get them to take cybersecurity seriously.

First, she had to raise executives' awareness of the phishing threat. To gain support, she calculated the cost of a single hypothetical ransomware attack delivered via phishing.

"I wanted to estimate what it would take to get from day one of a locker ransomware attack—which have become increasingly common—to a recovered position. I sized the man-hours for the recovery to be more than £250,000 [~\$350,000] for a single incident," said Marjoribanks. "When you start talking in monetary terms, people sit up and start listening."

THE SOLUTION

After assessing the different solutions on the market, Marjoribanks chose Proofpoint Security Awareness Training, formerly Wombat Security. She felt that Proofpoint offered "a technically superior product" and a tone that aligned with the bank's professional culture.

RBS selected the Anti-Phishing Training Suite, which combines customizable ThreatSim® Phishing Simulations, interactive training modules and robust business intelligence tools. The suite is administered through the Proofpoint Security Education Platform, a purpose-built learning management system (LMS).

Marjoribanks started with a pilot program that helped her work out details and engage stakeholders across RBS. Within a year, she was ready to roll out the program to all 80,000 users.

Ongoing phishing assessments and auto-enrolled training

RBS uses ThreatSim to deliver regular, ongoing phishing assessments, and uses email templates that emulate actual phishing lures spotted in the wild.

“Phishing has to be at the forefront of people’s minds. Even if we get to a point where we have an acceptable click rate, we just have to keep going.”

Lesley Marjoribanks, customer security manager and security awareness lead, RBS

The program follows a repeating, three-step pattern:

1. An initial simulated phishing email is sent to all 80,000 end users. Anyone who clicks on the email receives a Teachable Moment—a “just-in-time” message that lets the user know what they did wrong and how to avoid traps in the future.
2. Anyone who falls for the first simulated attack soon receives a second phishing test. Users who click on that second email receive another Teachable Moment, and are automatically assigned targeted, interactive training via our Auto-Enrollment feature.
3. Two-time clickers receive a third phishing email following the training assignment window.

At that point, the cycle starts again with a new campaign, assessing all 80,000 users. This continuous approach is a best practice for security awareness programs.

Leveraging expertise with managed services

As the program began to grow and achieve buy-in across the organization, RBS opted to use the Proofpoint Managed Services offering. “Initially, we started with a standard contract, and it was just me, essentially, doing it for 80,000 people,” said Marjoribanks. “We moved to a Managed Service contract, and that took the weight completely off me.” She describes her Managed Service Engineer as “essentially a remote colleague for me,” and appreciates the attention to detail the RBS program receives.

THE RESULTS

Overall, RBS has reduced its phishing susceptibility by more than 78% using the Anti-Phishing Training Suite. In the first two months alone, click rates fell from 47% to 22%, and now hover around 7-9%. These lower click rates also show the effectiveness of our approach to user education. Available in 35+ languages, our education content connects with users in their own languages—a must-have for global organizations like RBS.

In terms of ROI, the program has easily paid for itself by reducing the number of cyber attacks infiltrating the organization. RBS executives appreciate the solution’s robust business intelligence features, which provide insights that other security awareness tools cannot, including the ability to easily identify benchmarks and track progress.

Ultimately, Marjoribanks is glad RBS chose to go with Proofpoint “not just because we felt the product offered more than their competitors technically, but also because the user education experience had the edge with tone, pace, and multinational options,” she said. “The product itself is constantly evolving, and there’s always something new to offer our colleagues by way of education.”

LEARN MORE

For more information, visit proofpoint.com/security-awareness

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) is a leading cybersecurity company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.