CUSTOMER SUCCESS STORY

The Company - a leading financial services company with global reach

Payoneer empowers global commerce by connecting businesses, professionals, countries and currencies with its innovative cross-border payments platform. In today's borderless digital world, Payoneer enables millions of businesses and professionals from more than 200 countries to reach new audiences by facilitating seamless, cross-border payments. Additionally, thousands of leading corporations including Airbnb, Amazon, Getty Images, Google and UpWork rely on Payoneer's mass payout services. With Payoneer's fast, flexible, secure and low-cost solutions, businesses and professionals in both developed and emerging markets can now pay and get paid globally as easily as they do locally. Founded in 2005 and based in New York, Payoneer is venture-backed, profitable and ranked in the top 100 of Inc. 5000's Financial Services companies, and was ranked #13 on the 2018 CNBC Disruptor 50 list.

"We can actually see a correlation between the graphs and the results on the ground: When we run 'red team' drills, our employees now report phishing very quickly and you can see how this has become very important to them."

The Challenge - an industry under constant attack

The Financial industry is one of the top targets of hackers using phishing attacks to breach security, with access to customers' bank account or to the internal network of a financial institution perceived as striking gold. In 2018, phishing attacks skyrocketed in the financial services industry: over a third (35.7%) of phishing attempts were in the financial services industry, according to the Spam and Phishing in Q2 2018 report and this growth trend is expected to continue.

Yaron Weiss, Payoneer's VP Corporate Security and Global IT Operations, has been leading the company's security efforts since 2014. With steady increase in phishing attacks, Weiss realized the high-risk potential from Payoneers' insider threat - its employees.

Before learning about CybeReady in 2016, Payoneer used a different phishing simulation solution for its 1,200 employees for just one year. That solution required resources and training expertise that Payoneer's IT team didn't have, and despite the considerable effort that went into the program, it generated a total of two email campaigns in a full year. With random training efforts and no proper training methodology driving the process, employee behavior didn't seem to change.

The Solution - an autonomous training platform

When Weiss saw CybeReady's autonomous training platform product demo, he was immediately sold. "CybeReady's solution addressed all the challenges we were facing at the time," he said, "it is fully managed and offers each employee continuous training in their own inbox and their native language".

CybeReady utilizes a proven methodology, powered by Machine Learning. It offers a minimum of 12 phishing simulations to each employee annually, and it is customized, localized and adaptive to each employee' performance.

Weiss decided to switch to CybeReady within a week. Getting started was fast and easy - CybeReady offers a cloud solution that takes three quick steps and a total of one hour to integrate:

Export the company's address book

Whitelist a short list of domains

Approve 1st campaign

The Results: 7x increase in Employee Resilience Score

Weiss started noticing the difference in employees' behavior towards phishing attacks pretty quickly. Using CybeReady's real-time customer dashboard, he looked at two main KPI's:

1. Employee Resilience Score - more than tripled within the first six months and increased by over 7x over the two years of training with CybeReady.
2. Serial Clicker Rate - The Employee High Risk Group has converted to high performing as the % of serial clickers out of all employees was reduced to almost ~0%.

CybeReady also provides the Payoneer security team with weekly, monthly and quarterly reports they can easily share with Management. Payoneer's executives appreciate the robust business intelligence features and the ability to track progress.

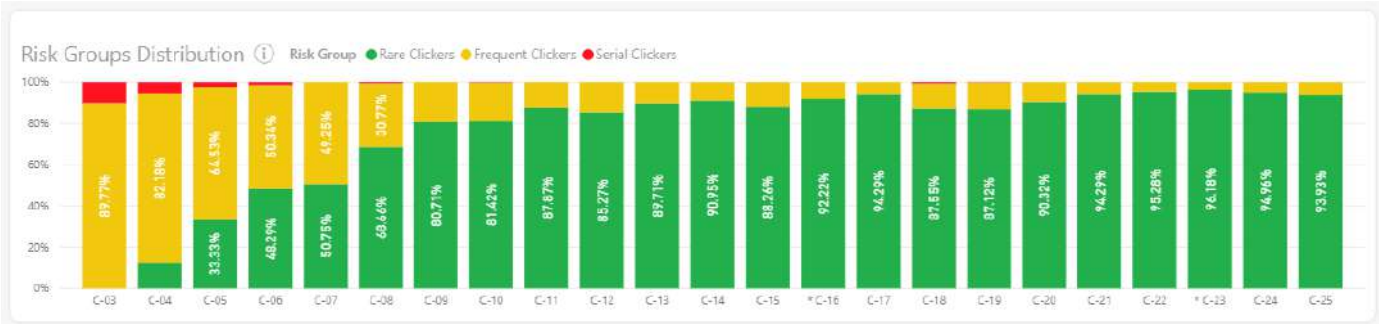
In addition to the progress seen "on the dashboard", Weiss indicated that his team noticed change in employee behavior "in real life": "We can actually see a correlation between the graphs and the results on the ground: When we run 'red team' drills, our employees now report phishing very quickly and you can see how this has become very important to them."

> **"since it's a fully managed solution, there's no effort required from our team and the results are significant. It feels like we've taken charge of our employee awareness and can better rely on our own people to make the right decision when faced with a phishing attack."**

Weiss pinpoints the key factors to a successful employee training program from his experience: "I've been using phishing simulations for Payoneer employee training for three years now," he said, " and I can say that the most important factor to success is continuity - training each and every employee month after month consistently and repeatedly".

In terms of ROI, the program has easily paid for itself. "We are paying the same as we did to the previous vendor, but getting significantly more value," said Weiss.

7x increase in Employee Resilience Score; Decrease in Serial Clicker rate



Significant change in Risk Group Distribution, with most employees converting to Rare Clickers