

CASE STUDY

IACC Professional Institute: A Complete Training Strategy with KnowBe4

[IACC Professional Institute](#), based in Chile, offers students asynchronous (recorded) remote learning. Its mission is to train individuals in technical and professional fields through online programs that satisfy various needs throughout their working life, promoting the continuous development of its students and the society in which they are involved.

Since the creation of their information security team in 2021, IACC has made cybersecurity and protecting the institution from possible social engineering threats a priority. After trying to develop a strategy with a provider that did not satisfy their business needs, they decided to search the market for a new provider who could offer them a complete and consistent strategy.

"In 2023, we received the recommendation from someone outside the institution who already used the KnowBe4 training and phishing resources that it would be the perfect organization to support us, and this was confirmed by an outside consultant we have. We conducted some free trials provided by KnowBe4, explored the ModStore resources and the available templates, and we decided to choose them," says Jaime Gacitúa, an Information Security Analyst at IACC.

Having a Strong Launch Strategy

During the first month of implementation of [KnowBe4's Security Awareness Training platform \(KSAT\)](#), the security team focused on completely familiarizing themselves with the tool. They received training to master their performance and explored all the simulated phishing templates available to design an effective internal launch strategy that would have a positive impact on employees.

"Since the beginning, we have had the backing of a KnowBe4 Customer Success Manager."

"Since the beginning, we have had the backing of a KnowBe4 Customer Success Manager. We had some concerns about users' participation in the training and we needed to design something that would capture their attention in the first session," Gacitúa says.

The first training session attracted 72% involvement out of a total of 320 employees. Immediately after, they conducted a phishing test to compare the results of the participants and those who did not

IACC Institute

Industry

Education

Headquarters

Santiago, Chile

Challenge

Improving security culture and user click rates on phishing emails.

Success by the Numbers

- 45% better results compared to the previous provider
- 72% employee involvement in the initial training
- 230 employees trained
- 25% clicks on the first phishing trial with KnowBe4

participate in the training. Of all employees, 25% clicked on this first phishing test after the initial KnowBe4 training session, which represented a 45% improvement compared to the previous provider.

Preparing Employees to Defend Against Suspicious Emails

Providing security awareness training about how to handle suspicious emails is a priority for the IACC information security team, and the KnowBe4 training sessions have been fundamental to supporting this mission.

"We are very satisfied with the content available in the ModStore."

"We are very satisfied with the content available in the ModStore. The first series we used was the one by Kevin Mitnick, and it was very well received by our employees. We thought it was very complete, since each subject was explained in detail through short videos the employees can watch on their computers during the work day. Also, everything is available in our local language, Spanish," Gacitúa says.

Each time an employee clicks on a simulated phishing email, they are automatically enrolled in additional training in order to prevent future incidents. Information on employee click rates is also included in a general report for management, which is in turn presented regularly to an institutional committee both monthly and annually. This allows the IACC team to track progress and compare the results of the initiatives and simulated phishing campaigns conducted.

Understanding the Tool to Improve Results

The first campaigns were directed to all IACC employees. For the next planned training sessions, the security team will segment out testing and training for the group of new employees and those who have never participated in a previous session. Subsequently, they will be segmented by key departments like human resources, admission and finance.

"This year we brought in many new employees, a total of 206 in 2024, which requires us to maintain an ongoing training and awareness process for everyone. We always

focus on reviewing the results to plan the next steps, and now we are considering the implementation of short-term courses directed at employees with more training," Gacitúa says.

In addition, IACC is evaluating the implementation of [AIDA](#) (Artificial Intelligence Defense Agents), the KnowBe4 artificial intelligence tool, for the next phase of training. AIDA will assist the institution in dynamically selecting phishing test templates and automatically give optional learning recommendations based on users' knowledge and skill level.

Reaping the Benefits of an Engaged User Base

Understanding how employees perceive and accept security awareness training is crucial for IACC, which constantly pays attention to their responses. Acceptance has been positive, with employees emphasizing that it is an effective way to be alert to possible threats. They believe it is very comprehensive, easy to use and interactive.

"KnowBe4's platform easily exceeds the common messaging organizations frequently offer; it is the best tool to raise users' awareness about cybersecurity and potential social engineering threats."

From the information security team's perspective, the benefits are notable. The broad offering of training content contributes to reducing clicks on phishing emails, while the interactivity of the ModStore increases involvement.

"We are very pleased with our collaboration with KnowBe4. It is a very comprehensive platform where you can find everything necessary to train and evaluate users. KnowBe4's platform easily exceeds the common messaging organizations frequently offer; it is the best tool to raise users' awareness about cybersecurity and potential social engineering threats," Gacitúa says.