Case Study

Desktop Structures Cybersecurity Department on KnowBe4 Platform

DESKTOP

Industry

Telecommunications

Headquarters

Sumaré,
São Paulo, Brazil

Challenge

To set up the foundation of a cybersecurity program and a culture of security awareness

Desktop's history began in 1997, when the organization's current shareholder founded Desktop Online Informática. Since then, the organization has gained thousands of subscribers and provides internet connection services in cities across the state of São Paulo, Brazil.

After going public in 2021, Desktop needed to improve its information security business processes. This led the organization to create a specific cybersecurity team responsible for deploying training programs and implementing a cybersecurity culture among its employees.

Recognition, Accessibility and Content Were Crucial to Choosing KnowBe4

To help achieve this goal, Desktop began evaluating platforms that could manage cybersecurity training for employees. After researching various products, the organization chose to implement KnowBe4's Security Awareness Training and Compliance Plus Training.

At a Glance

- Employee trainings launched every two weeks
- 88% employee completion rate on the trainings
- Training delivered to almost the entire organization
- Reduced phishing email click rates through continuous simulated phishing tests

Luiz Barbosa, Cybersecurity Specialist at Desktop, said that the organization considered vendor reviews carried out by renowned research institutes, such as Gartner™, which ranked KnowBe4 among the leading platforms for security awareness training. Barbosa also highlights the volume of content, frequency of updates, and the simplicity of the KnowBe4 platform interface as key factors for choosing KnowBe4.

"The accessibility offered through captioned video training is another major factor, especially when it comes to an organization that seeks social inclusion, as is the case with Desktop," Barbosa says, adding that the organization currently has employees with hearing impairments.

> *"The accessibility offered through captioned video training is another major factor, especially when it comes to an organization that seeks social inclusion, as is the case with Desktop."*
>
> *— Luis Barbosa, Cybersecurity Specialist, Desktop*

Accurate Diagnosis for the Implementation of a Security Culture

As soon as Desktop implemented the KnowBe4 platform, the organization carried out the Security Culture Survey (SCS) and the Security Awareness Proficiency Assessment (SAPA). The SCS facilitated Desktop's risk management by assessing the current state of security culture across the organization. The SAPA provided an overview of the organization's security strengths and weaknesses based on assessing the user's security knowledge. Barbosa said the results of both surveys played a key role in establishing Desktop's training strategy.

To complete the diagnostic process, the organization carried out a simulated baseline phishing test and found out the percentage of users that would click on a real phishing email attack.

"The diagnosis helped us to identify our weaknesses, and gave us direction as to what our first security awareness trainings should be," Barbosa says. "Two subjects—passwords and authentication and incident reporting—scored below 50% among the users who took part in the initial test. Based on that, we focused our first campaigns on these topics."

88% Employee Training Completion Rate with KnowBe4

In May 2023, Desktop began providing training to its employees through the KnowBe4 platform.

All of the employees receive new training every two weeks. Barbosa explains that, by default, the KnowBe4 platform requires training to be completed within 30 days. Desktop, however, has been seeking to streamline this process.

"Initially, we are working so that the training can be carried out in 20-25 days, at most," he says. "We set up the system to send emails with the training deadline period and request that the employees complete it as soon as possible."

Training can also be accessed through the KnowBe4 Mobile Learner App, which helps increase the training completion rate, as it allows employees to access the content anywhere and at any time.

Barbosa says the strategy has been successful thus far. The organization has reported an average of 88% completion in the training.

"We are aware that there are always employees who are on vacation or leave, which makes it difficult for us to reach a 100% rate," Barbosa says. "Still, we are working with managers to further engage employees and help increase this rate."

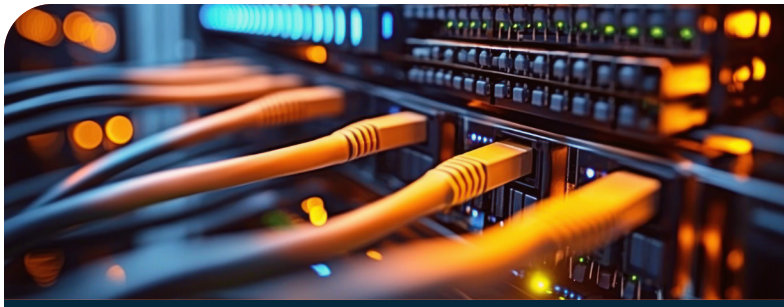
Phishing Awareness Carried Out in Parallel

Alongside the training, Desktop sends phishing simulations every 15 days. Barbosa says that the KnowBe4 platform automatically creates campaigns using different templates. "A schedule was developed, with emails sent to employees in an automatic and random manner," Barbosa says. This makes it easy to test employees on a regular basis and understand the risk of them clicking on a phishing email.

The Desktop team monitors the results through reports generated by the KnowBe4 platform and, based on these analyses, identifies those employees who are characterized as repeat offenders.

"For those who click more than once on phishing simulation emails, we set up specific training campaigns that are mandatory for those employees to complete the additional training," Barbosa says.

Barbosa says the click rate of emails in phishing simulations has decreased with each new test.



"The diagnosis helped us to identify our weaknesses, and gave us direction as to what our first security awareness trainings should be."

— Luis Barbosa, Cybersecurity Specialist, Desktop

Desktop also implemented the Phish Alert Button, a phishing alert icon added to their email platform users can click to forward suspicious messages for analysis by the cybersecurity department. "The use of the Phish Alert Button has increased significantly with the training," he says.

Foundation for a Robust Organizational Culture in Cybersecurity

Since implementing the KnowBe4 simulated phishing and training platform, Desktop has strengthened its overall security posture.

Barbosa notes that a large number of employees gave positive feedback regarding the platform, praising the quality and variety of content, as well as its direct impact on the organization's business and image.

"Desktop's board, managers and even shareholders are noticing this greater security awareness among employees," he says.

"KnowBe4 is playing a key role in promoting a robust organizational culture in cybersecurity through its phishing testing and training," Barbosa says. Additionally, he says KnowBe4's phishing simulations have been crucial in assessing the organization's resistance to external threats, something that is fundamental for the longevity of a business.

What's Next: Targeted Training and More Automation Against Phishing

After almost a year of the same training for all areas of the organization, Desktop will begin targeting training content specific to each department in the coming year. "Initially, we are structuring specific training for the areas of Human Resources, Development and Finance," Barbosa says.

The organization also plans to deploy episodes of KnowBe4's award-winning series "The Inside Man." "The Inside Man" educates and entertains with streaming quality episodes that tie security awareness principles to key cybersecurity best practices.

Desktop is also considering expanding the number of licenses available to serve new employees, and implementing PhishER Plus to automate the prioritization of phishing messages and expedite responses to these threats.

> *"KnowBe4 is playing a key role in promoting a robust organizational culture in cybersecurity through its phishing testing and training."*
>
> *— Luis Barbosa, Cybersecurity Specialist, Desktop*

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com