KnowBe4

CASE STUDY

Strategic and Smart Security Awareness With Capitec

Capitec, a leading financial services organisation with a significant footprint, recognised the importance of a robust employee awareness programme to reinforce its security footprint and transform how employees engaged with security training and awareness. The company spent six years focusing on its awareness journey, investing into training solutions and systems to try and engage with a diverse workforce, but transformed this in less than a year with the KnowBe4 platform.

According to Juan-Marc Scrimgeour, Acting Head: Technology Security at Capitec, the company's strategy took four factors into consideration: the risk profile of the area; the awareness gap within the area; the current environment, and the macro and micro impacting factors; and the format best suited to deliver the training.

"Our strategy has moved from a face-to-face training approach to a more digital, multi-pronged awareness training strategy. We use the KnowBe4 platform and the Smart groups to create a granular awareness strategy that allows us to send customised training to various staff groupings in various, relevant formats."

The team set out on this security journey because it recognised the importance of implementing a wider security strategy for the financial institution, a strategy that encompassed all levels and layers throughout the organisation. The security team realised the importance of reducing threats from within the environment and providing an extra layer of security by engaging with the people who worked there.

"The human layer is so important," says Scrimgeour. "Controls can be bypassed, systems can be fooled but there is a person at the end of the attack, and we need them on our side to help us. We realised early on that people often don't know enough about cybercrime, or misunderstand what certain threat actors do or mean, and that to improve our security culture, we had to focus on our people."

The Requirements

Initially, the team hit resistance with middle management and this limited uptake of the training. Without the middle management teams driving the training processes, it was difficult to get employees to finish their training and develop their understanding of cybersecurity. This was further complicated by the fact that many employees didn't know what they were supposed to do when faced with a threat, and that many were becoming the security problem.

"The directors of the company wanted more emphasis on security, and we needed to fill in the gaps that were currently impacting on our development of a truly robust security posture," says Juan-Marc.

> *"Our strategy has moved from a face-to-face training approach to a more digital, multi-pronged awareness training strategy. We use the KnowBe4 platform and the Smart groups to create a granular awareness strategy that allows us to send customised training to various staff groupings in various, relevant formats."*

The company had limited training content, which impacted on engagement, and both reporting and escalations of incidents were manual. The training systems didn't have any simulation capabilities and was in a one-size-fits all packet, which meant it didn't really deliver what individual people, siloes and business units needed. Some employees wouldn't understand the training, and it wasn't done often enough to embed security best practice into their behaviours.

"Our old systems weren't short and easy to consume, they weren't granular enough, and they didn't have the right structure for proper learning," says Scrimgeour. "We needed a platform that would serve relevant information at regular intervals in formats that were understandable and that fit the person and the environment."

What Success Looks Like

The KnowBe4 platform ticked several boxes for the Capitec team. It was easy to use and manage, it had AD integration and support for solution queries and issues, it was locally supported, it included simulations and reporting capabilities, it provided the company with access to a large content library, and it could be accessed from anywhere.

"We had already partnered with Popcorn Training to help create and facilitate awareness training in the company, so when they were acquired by KnowBe4 and introduced us to the platform, the move made sense," says Juan Marc. "We did look at other providers, all were assessed on the criteria above, but the KnowBe4 platform was the right fit for what we needed."

> *"The phishing simulation programme is fantastic—not only did we automate the simulations completely, but the templates are updated on a regular basis and sent out based on a preset difficulty level so training is relevant and ongoing."*

Capitec invested into the Diamond license that provided them with access to all the content on the KnowBe4 catalogue including free tools, phishing simulations and KnowBe4's Phish Alert Button. The team spent very little time implementing it and educating teams on how to use it. It was the size of this catalogue and the ease of deployment and user management that cemented the deal.

"The platform was really easy to use, we could set it up and create granular awareness training streams for various groups based on specific attributes," says Scrimgeour. "The phishing simulation programme is fantastic—not only did we automate the simulations completely, but the templates are updated on a regular basis and sent out based on a preset difficulty level so training is relevant and ongoing."

It took just over a month for the team for implementation, launching in January 2019. Since then, the platform has reduced the manual and operational burden on the security team substantially, and has made it easy to create and deploy granular awareness campaigns. Awareness is always relevant and takes external factors into consideration without adding to anybody's workloads.

"There has been a significant increase in phishing reporting, in users questioning policies and alerts on their devices, and often identifying risk emails or threats that were missed by security systems," concludes Juan-Marc Scrimgeour. "We can't control who attacks us, and when, but we are creating a secure and engaged workforce that understands the risks and plays a role in ensuring the ongoing security of the organisation."