KnowBe4

CASE STUDY

Fashion Marketplace

About Depop

Founded in 2011 by Simon Beckerman, Depop is a peerto-peer, global fashion marketplace with over 27 million users buying, selling and connecting. Headquartered in London, the company is over 300 employees-strong and have offices in the United Kingdom, Australia, and the United States, specifically New York and Los Angeles. The mobile app adopts a layout similar to social media and encourages individuals to sell and buy unwanted items; in this way, endeavouring to make fashion more sustainable.

Getting the Ball Rolling

When Pedro Borracha, Head of Information

Security at Depop, first joined the company in July 2020, to build the company's informational security team. As such, Pedro spent his initial three months investigating Depop's security posture. He ran penetration tests, conducted security assessments of Depop's cloud environment and organised a thorough audit with PwC.

On the back of this audit, Pedro needed to create a roadmap and it became clear that security awareness training as well as the documentation of policies and procedures were of top priority.

Unfortunately, he also had to contend with an extremely busy workforce as most employees felt they did not have sufficient time to dedicate to security awareness training. He needed help transforming this mindset and reinforcing the idea that cybersecurity is everyone's responsibility. He needed the business to understand that cybersecurity training should be undertaken as part of employees' job roles, during business hours.

Decisions, Decisions...

Pedro was familiar with KnowBe4, having successfully implemented the training at a former company. Nevertheless, he decided to do his due diligence and assess other options prior to committing. Yet, he quickly found that KnowBe4 offered, by far, the best option.

KnowBe4 excelled particularly on two fronts: user experience and an unmatched repository of training materials and phishing templates.

"I tried to think, not as an admin of the platform, but as a user, and everything was clear. The user experience and interface are second to none, and I can say this, because I've looked at all the competitors," shared Pedro. "The second thing is the ModStore. The amount of material that we have access to and can distribute for training is again, second to none."

While in the beginning, general training modules were issued to everyone, this has now evolved, becoming customised to roles and departments.

He adds: "With the plethora of training available, we can customise to the needs of each department. As far as I know, KnowBe4 is the only company that has so much choice that you can nit-pick exactly what you want for each team – and we have a lot of teams."

By simply leveraging KnowBe4's filter function, Pedro and his team of three, can "nail down exactly what we need" – length of video, subject matter, whether the modules are interactive or not, etc. – in a matter of seconds. The same can be said about KnowBe4's simulated phishing feature; everything from who and when someone gets a phishing email to how it looks, can be fully tailored to their needs.

Time To Make an Effort, Not an Excuse

Since using KnowBe4, the company mindset on security awareness training, and cybersecurity more generally, has done a 180. Through gamification and the platform's leaderboard, employees have become inspired to engage in a bit of friendly competition. Through notifications, Pedro can also inform managers if their teams are falling behind.

"In the beginning, people will say: What is this training? Is this optional? Is it mandatory? I'm too busy. I know all the excuses. But KnowBe4 has allowed us to slowly but surely, transform training into something that is welcomed," Pedro affirmed. "We have successfully distributed policies via KnowBe4, too. Just this morning I sent out an acceptable use policy and in just over an hour, 81 employees have already acknowledged it. That is one person per minute. When we first started, this would have been unthinkable."

KnowBe4 is now very much embedded into Depop's cybersecurity maturity roadmap and it is used daily for training campaigns, phishing exercises as well as reports submitted to the executives on a weekly basis.

What's more, if there is ever something Pedro wished KnowBe4 could do to improve their offering or if he needed help resolving an issue, he knew he could depend on his customer success manager to make it happen.

"I have full faith that if I send an email to my customer success manager, I will get a reply in less than ten minutes," said Pedro. "They really listen and follow through."

Overall, Pedro believes that Depop's return on investment with KnowBe4 is critical to circumventing external threats. In only eight months, he has seen a 20% decrease in the number of people falling for a phishing scam. Following a baseline campaign in December, Depop's Phish-To-Click (Phish-Prone percentage) ratio was at 29%, this then dropped to 17% in January, then 9.8% in February. With every week of training, Pedro is seeing a clear reduction in the risk.

A Word of Advice

"I would definitely recommend KnowBe4. However, one thing I would suggest companies do before committing is to do a demo. Make sure that you understand all the technical requirements and speak with your IT department to ensure that your systems are compatible. While it's certainly not a deal breaker, failing to check could result in some delays during the implementation process. For example, we use Gmail which tends to blacklist all of our simulated phishing emails. This is not a problem with KnowBe4, but it is something to be aware of so that it can be resolved swiftly and early on," Pedro explained.

"Overall, Pedro believes that Depop's return on investment with KnowBe4 is the cost of a breach."

What's Next?

In terms of future plans, Pedro and his team expect to implement USB security tests when employees eventually return to the office. Users will see USB sticks randomly placed around the office, and the team will monitor if any files are opened by staff.

They also hope to assign corporate mobile phones to all employees to have full control over the security of these and the confidential data held on them. Once this is in place, Pedro and his team intend to issue simulated vishing – voice phishing, a common tactic for social engineering - training as well.

"While we still have some way to go to improve our cybersecurity posture, with KnowBe4 we are taking the right steps to get there. I'm a big KnowBe4 fan," Pedro concluded.