

## CASE STUDY

## Gamifying the Way to Phishing Resilience at Whitbread

Just weeks into her new role as information security awareness and communications manager at the multinational hospitality company Whitbread, Elise Mutch knew what she wanted.

Mutch already had years of experience in the security awareness industry, specifically in the realm of simulated phishing. Her goal at Whitbread: use her knowledge of targeted training and assessments to lower user click rates, change user behavior for the better and support an overall security culture.

“I’ve been known as the phishing queen,” Mutch says.

Mutch came into her position to find the KnowBe4 training and phishing platform already implemented, but at a limited capacity. Mutch had worked with KnowBe4 at a previous organization and knew the success the partnership could bring to Whitbread. Her focus at Whitbread is 1,500 support center staff who had been receiving unfocused phishing campaigns with no clear baseline to measure success.

### Setting the Baseline

Mutch decided to start from scratch and use the KnowBe4 platform to send a medium-difficulty phishing email to the 1,500 users to gauge their phishing susceptibility. Mutch said the pre-built KnowBe4 phishing templates with star-based difficulty ratings made it easy for her to choose the correct templates for her first campaign.

The results from this first test presented both good and bad news. The Phish-prone™ Percentage (PPP)—the percentage of users likely to click on a phishing email—was strong at only 5%. However, Mutch found the percentage of users reporting messages to be only 2%, despite having KnowBe4’s Phish Alert Button (PAB) installed in their email client. The PAB allows users to report suspected phishing emails from their inbox straight to the infosec team with one click.

## Whitbread

### Industry

Hospitality

### Headquarters

United Kingdom

### Challenge

Low simulated phishing email report rate

### Success by the Numbers

- Users reporting simulated phishing emails increased from 2% to 31% in less than a year
- Improved communication between users and the infosec team
- Nearly a quarter of users participating in the inaugural phishing tournament, raising user engagement with security training and simulated phishing

Mutch used the KnowBe4 platform's capabilities to assign those who had clicked on the phishing test to a brief training with built-in quizzes to underscore the importance of knowing what a phishing email looks like. She also built custom communications to help spread the word about the PAB and how to use it.

"Anything short of neon arrows going 'Click here,'" Mutch says.

### User Confidence Grows

A few months later, her work paid off. Another slightly more difficult phishing campaign resulted in a similar PPP but a 25% report rate, compared to only 2% previously.

---

*"That's the goal, for them to feel more comfortable about recognizing the signs of a phish," Mutch says. "One of the values of Whitbread is confidence, and I want to give them that confidence to recognize an infosec incident."*

---

Mutch was thrilled to see such a significant increase in reported emails because it meant her users were becoming more confident with the correct actions to take when presented with a potential phish.

"That's the goal, for them to feel more comfortable about recognizing the signs of a phish," Mutch says. "One of the values of Whitbread is confidence, and I want to give them that confidence to recognize an infosec incident."

### Gamifying Cybersecurity Awareness Month

October is well-known as Cybersecurity Awareness Month for many infosec professionals around the world. It's a time to promote cybersecurity best practices for weeks in a row with webinars, special events and whatever the cleverest of security awareness managers can think up.

During her first October with Whitbread, Mutch wanted to go big. She had success with simulated

phishing tournaments in her previous role and knew she and KnowBe4 could make it happen again.

Mutch put together a multi-week phishing tournament comprising four topics (such as fake invoices and CEO impersonations), nine rounds and 2,000 specially crafted phishing emails; plus Amazon gift cards and branded office supplies for the winners. She used the KnowBe4 platform's Smart Groups feature to organize the different phishing campaigns based on how users responded.

"By using the KnowBe4 platform, it gives the best chance of success," Mutch says. "Smart Groups is where it's at."

Mutch used the Smart Groups feature throughout the month to customize messaging for users who had progressed successfully by reporting phishing emails. She also tailored the pop-up messages for the PAB for the entire month to align with the broader campaign themes.

---

*"Once they click that [phish report] button, they've got that recognition right in front of them," Mutch says. "They love it; it's gamification and it raises engagement."*

---

With the success of the tournament, the phishing report percentage increased from the original 2% baseline to 31%; the highest Mutch had yet seen.

"Once they click that [phish report] button, they've got that recognition right in front of them," Mutch says. "They love it; it's gamification and it raises engagement."

Mutch said she received positive feedback throughout the tournament, mainly through the dedicated email inbox her team set up for questions or comments from users.

"It was great to take part; it definitely kept me on my toes!" one user shared with Mutch.

Mutch found the best proof of success in a more open line of communication between her users

---

*"[I've raised] the level of engagement through this tournament, and I couldn't do the tournament without KnowBe4," Mutch says.*

---

and the infosec team. Her users would use the dedicated inbox to say certain phishing emails were too easy or ask questions about other cybersecurity topics; resulting in 150 total messages throughout the month.

"[I've raised] the level of engagement through this tournament, and I couldn't do the tournament without KnowBe4," Mutch says.

### **First Year Success and the Future**

With more reported phishing emails and increased communication with the infosec team, Mutch said she sees both the qualitative and quantitative improvements as proof that her focus on behavior change and assessment through simulated phishing works. Not to mention, her CISO has authored bigger and better prizes for next year's phishing tournament.

"My first year I would say has been a success," Mutch says.

In the near future, Mutch said she wants to make better use of KnowBe4's "Point of Failure" video training landing page templates, which include videos that focus on various topics specific to cybersecurity training. She would also like to incorporate more KnowBe4 training on other cybersecurity topics.

---

*"As long as everyone does their little bit, they can all be secure together," Mutch says.*

---

Overall, Mutch feels the simulated phishing campaigns play a significant role in reminding her users of the vital part they play in Whitbread's overall security culture.

"As long as everyone does their little bit, they can all be secure together," Mutch says.