DISCUS SYSTEMS plc

SECURITY TRAINING

brigantia

Why do we do training and phishing simulations?

It is difficult to change user behaviour in a positive and permanent way without providing ongoing training. It is only by doing training on a regular basis that users have security at the forefront of their minds. One training campaign is allocated to each user every three weeks (the average duration of each piece of training is only five minutes).
Phishing simulations are run weekly to keep users on the lookout for phishing emails. Since the process is completely randomised, users
all get different emails and at different times, so they cannot warn each other when a phishing simulation email is spotted. As the users are always looking for these phishing simulations, they spot any real-world phishing emails too.

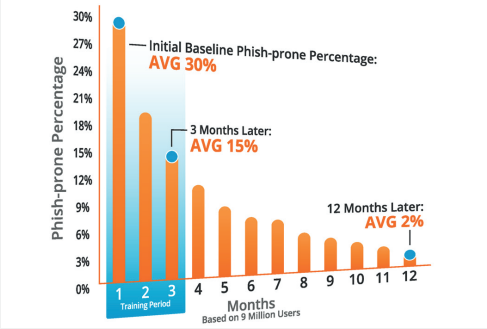
Training

- Users will receive email notifications from KnowBe4 (do-not-reply@knowbe4.com) with a login link.
- We can brand these emails to ensure trust, and recommend informing staff about the training (template available).
- KnowBe4 uses Single Sign-On or a Password-less link, so no account creation is needed.
- The training platform clearly shows required training and deadlines.
- Training ranges from light-hearted scenarios to specific technical modules.
- Reminder notifications will be sent every five days until training is completed.

Phishing Simulations

- If a user clicks on a link or opens an attachment, then training will be allocated immediately to teach that user the skills required to easily spot phishing emails.

Did you know that 91% of successful data breaches started with a spear phishing attack?



u2us@discus.co.uk | 01675430080 | Patrick Farm Barns, Meriden Road, Hampton in Arden, Solihull, B92 0LT