CASE STUDY

20% of Employees Clicked Simulated Attack Email

ADAMS BROWN
Technology Specialists
above+beyond

The challenge:

A 100-person company was concerned with its cybersecurity and the technology proficiency of its workforce. Company leaders were afraid limited cybersecurity awareness among employees posed a significant risk to the company and its security.

The resolution:

As part of a cybersecurity assessment, we ran a simulated phishing attack. The results were:

Over **50%** of the team opened the simulated phishing email

20% of employees clicked on the malicious link in the phishing email

Thankfully it was merely a simulation! However, the exercise highlighted the ease with which a malicious actor could seize credentials and potentially dominate the system. Consequently, this revelation prompted the creation of a comprehensive priority roadmap that demanded urgent attention.

The impact:

Company leaders have initiated monthly cybersecurity training sessions for all employees, educating them on potential threats. Concurrently, monthly phishing tests continue to be conducted. Within six months, the click-through rate on these tests plummeted to less than **2%**, representing tangible progress and a significant reduction in the company's risk profile.