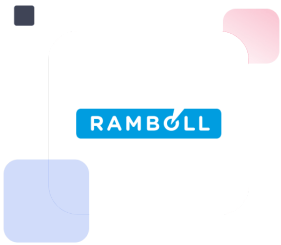
CASE STUDY

Ramboll educates employees on email-based threats with Hoxhunt



About

Headquarters: Copenhagen, Denmark

Offices: in 35 countries

Employees: 17,000

Challenge

Traditional security awareness training didn't result in the desired failure rate and scalability.

Solution

Improve security engagement among employees that helps to integrate people into the company's defense

strategy better.

Cybercrime has exploded in recent years. Cyberattack tactics are becoming more sophisticated and their effects can cripple companies by causing severe financial loss or reputation damage globally. For Ramboll, a global engineering, architecture, and consultancy company, the focus on security has included maintaining its ability to function, enable safe operations, run secure IT systems and applications, and safeguard the data the company uses and collects.

The Challenge

Phishing is one of the top threats for organizations, and preparing employees against attacks with a security awareness program is thus imperative. Before Hoxhunt, Ramboll used a more traditional security awareness program that did not produce a sizable benefit. Ramboll management tested employee awareness and discovered a large fail rate. Hence, they charged the security team needed with establishing a dynamic security awareness training program that would train users to recognize potential threats, and instill behaviors that would help them avoid falling victim to attacks like phishing and, as a result, protect Ramboll's information and data.

The Solution

Ramboll chose Hoxhunt as their phishing training tool to teach employees to recognize suspicious emails from attackers. Ramboll decided to work with Hoxhunt for its ability to deliver education to employees that is interactive, personalized, and integrated into their everyday workflow. All these can help to improve security engagement among employees that helps to integrate people into the company’s defense strategy better.

Phishing scams use emails to lure employees to make an error that could help scammers gain access to systems. With Hoxhunt, Ramboll educates employees on phishing emails, social engineering tactics, suspicious links, dangerous attachments, and untrustworthy sources to remain protected from malware and ransomware attacks.

The Results

The phishing simulation program's goal is to provide employees with a safe, simulated environment where they can learn about what real phishing attempts look like in the wild. Since the start, Ramboll users have completed over 100 000 simulations with outstanding success rates. With Hoxhunt, Ramboll has significantly decreased the failure rates over time. As Hoxhunt adjusts the difficulty level to match the skill and knowledge level of each employee, the failure rate is more meaningful as it provides a more realistic picture of how people perform.

As a result of the training, Ramboll employees are comfortable identifying phishing emails through the phishing simulation program. The company's fail rate corresponding to the simulations is less than the global statistics that Hoxhunt provides.

The employees are excited to participate in the training and spot phishing emails. Initially, people were a little apprehensive about the training program, but the internal communication helped them understand the benefits of using Hoxhunt. The security team has also received emails from employees who wanted to increase the training's difficulty level to further develop their skills in recognizing actual phishing emails.