CASE STUDY

How agricultural technology leader, Kverneland Group sewed awareness training and reaped resilience

About

Kverneland Group is an

international company developing,

Challenge

To achieve their

aggressive goals of virtually

Solution

Four years ago,

Hoxhunt was selected for its next-level

producing and distributing agricultural implements, electronic solutions and digital services to the farming community.

Industry: Agricultural manufacturing, Sales & Distribution and IT

Location: 10 Production locations in 8 countries

Founded: 1879 in Norway

Employees: 2,623

onboarding all computer users in an ongoing cybersecurity training program, Kverneland Group sought an automated solution with a managed service component that would produce sustainable results.

automated phishing simulation platform and its customer success team, which have together maintained user engagement and performance at extremely high levels for an exemplary resilience score of 24.75.

KEY TAKEAWAYS:

“We have stayed with Hoxhunt for all these years because the product is constantly being updated, the content is always changing, and the phishing simulations actually get harder based on how the user performs. People continue to learn and they are motivated to participate with the way Hoxhunt gives stars and shields for successful behaviors.”

“What also really stands out is that when I give Hoxhunt feedback, something happens. We see the feedback integrated into the product. You don’tget that when you're working with the giant companies."

--Bård Berntsen, Director Group IT

Results

Kverneland Group boasts exemplary levels of user skill, participation, and performance, translating to outstanding organizational risk posture across the board; particularly considering the wide distribution of corporate sales and factory sites in over 17 countries.

- Resilience: 24.75. Resilience is the engagement rate divided by the fail rate. Any score above 12 is considered good. *24.75 is stellar*.
- 87.8% onboarding rate for whole company:
- 10 countries have onboarded 90 – 100% of employees. *Outstanding program management results.*
- 10,522 completed simulations
- 81.8 % engagement rate for whole company. *Outstanding results.*
- 68.1 % success rate. *Excellent.*
- 3.3 % fail rate. *Excellent.*
- 28.6 % miss rate. *Extremely low; excellent.*

Why Hoxhunt?

Kverneland Group started using Hoxhunt four years ago. Bård Berntsen, Director Group IT, noticed a shift in the quality and danger of phishing emails, which went from poorly crafted and mass-produced to clever and targeted. He knew that his main job was to prevent breaches, and most breaches would come from those evolving phishing attacks.

Kverneland Group selected Hoxhunt over competing options because it checked all the boxes. Where others required resource-intensive manual administration of templates, Hoxhunt enabled frequent, ongoing, personalized training at scale—with minimum resources. Berntsen wanted a solution that would help change culture and behavior. Hoxhunt promised such a result with its adaptive learning model, in which simulations would get harder or easier based on the user's skill level and progress.

He was also drawn to the positive reinforcement approach. People build skills when they are rewarded for success and motivated to learn from failure. It's about carrots, not sticks.

"In IT and security, we have way too much to do, and keeping up with security is such a big job. Security people are hard to find and we don't want the ones we have to sit and administrate a system like this; we want them to work on security. You could look at Hoxhunt as a completely outsourced awareness training service."

Why stay with Hoxhunt?

Hoxhunt has grown as a product and as a company along with Kverneland Group's cybersecurity ambitions. Languages have been constantly added to the training program, along with straight-from-the-wild simulations and new features and updates. It altogether keeps the training experience fresh and interesting for all users—hence their exceptionally high engagement rate of 81.8%.

"Language was an important part of this. When we localized language (like for our French users) that really got things in place. You have improved your system and we have improved our data."

Moreover, Kverneland Group has a high participation rate in Spicy Mode, the ultimate level of phishing training. Users must opt-in to Spicy Mode, where they receive the most targeted phishing simulations possible, reflective of the nastiest attacks in the wild. Last year, for instance, they customized an extremely hard-to-spot simulation during the budget process for the finance team that got a number of fails. Which was good: being challenged is important, as is being able to learn from failure in a safe environment. Interestingly, employee feedback has been positive even for these challenging simulations.

"What we see is that the longer we run this, the trickier it needs to be or else you don't get a fail rate at all. And that is where the spicy mode comes in. We don't force users into this but quite a few have joined on to Spicy Mode and job-specific customization… If you get a highly targeted spear phish you will get a higher fail rate."

Working with Hoxhunt

Berntsen praised the Customer Success team's energy and communications skills for keeping the training program on track. At their quarterly meetings they analyze performance metrics, give and receive feedback, and go over product updates have been ingrained into corporate communications practices. It's also been a great way to brainstorm ideas. For instance, Kverneland Group announces each quarter in a newsletter the best Hoxhunt user, who receives a diploma and a prize. Indeed, the country-by-country leaderboards have been well received as an effective way to motivate participation with healthy competition.

“We are doing different things to get more people active, and a lot of those things are coming from you and (Customer Success Manager) Kirsi. You have been very supportive on this journey.”

Evolving threat landscape demands a dynamic training solution

The cost of a phishing breach averages millions of dollars per company, per breach, according to Ponemon Institute research. Email-originated breaches can result in the delivery of malware or ransomware, the theft of credentials and data, or the redirection of funds into scam accounts. Breaches drain employee productivity and brand credibility. And, as Berntsen has seen, attacks are becoming more sophisticated by the year.

“The attack business is really developing quickly into very targeted and sophisticated campaigns, and that is really scary. The most we can do is to prepare people and make them aware that these attacks are happening. All the technical security in the world can’t really stop an attack from getting to an inbox or prevent a user from doing something wrong if he or she isn’t prepared.”