NINJIO

# CASE STUDY

## DHS SIMULATED PHISHING ATTACK ON CRITICAL INFRASTRUCTURE

| ANNUAL REVENUE | REGION | COMPANY SIZE |
|---|---|---|
| **$4.5 B** | **SOUTHWEST U.S.** | **25K EMPLOYEES** |

## DHS LAUNCHES A SIMULATED PHISHING ATTACK THAT RESULTS IN A .17% CLICK RATE.

**1** in **600** fell for a **DHS** crafted simulated **phishing attack** on a **NINJIO Critical Infrastructure client**

According to CyberGRX Security Analyst, Brianna Groves, the top 5 security threats for today's businesses are ransomware, phishing, data leakage, hacking, and insider threats. Furthermore, these threats continue to grow in frequency and scalability, as bad actors create new and innovative ways to penetrate even the most secure systems. Why? Because, generally speaking the problem isn't with the technology, it's with the people. In fact, according to Verizon's 2018 Data Breach Investigations Report, "93% of data breaches are caused by human error."

With no formal security awareness solution and faced with increasing threats of cyberattacks on large organizations, a leading global Consumer Packaged Foods company decided it was time to take the plunge. After meeting with NINJIO in the summer of 2016, the organization agreed to sign-on for a year. If the employees and staff genuinely engaged with NINJIO's content, and simultaneously gained the knowledge and education to make them viable "defenders against potential hackers", the partnership would continue.

> ***NINJIO** offered something **we hadn't seen before.** As a company, they were nimble; and their **solution was creative.** They listened to our specific concerns and vision for **creating a security aware culture.***
>
> **Bill F. -** Director of Technology & Governance

## THE SOLUTION

NINJIO Private Portal leveraging NINJIO AWARE Anime Episodes

Since 2016, the organization has remained a NINJIO customer, and has seen tremendous results with NINJIO's AWARE Anime solution. According to the Director, "We understand that the most susceptible part of the organization lies with the human element, and we have made so much progress in educating our employees: ultimately becoming a much more mature company in terms of security."

This security mindset is possible because 1500 of our associates are committed to watching NINJIO's monthly videos, completing the quizzes, and consuming the supporting content that NINJIO provides. They have subsequently adopted a NINJIO mentality of reporting suspicious activity (emails, etc.), and anything else that doesn't look right from a cybersecurity perspective.

"I hear people referencing NINJIO episodes constantly," continues the Director. "After an episode is released, co-workers will talk about it with each other. Everyone seems to have a heightened level of awareness and acknowledgement of potential threats." As a global leader in the food and beverage industry and consumer packaged goods, the organization's importance to food supply does not go unnoticed.

As such, the organization was classified as a "critical infrastructure" organization making it eligible for free programs provided through the DHS with respect to cybersecurity. This includes internal and external penetration testing, network security audits, and other solutions related to ensuring that their network, and their people, are secure.

> *But the real test came when the organization partnered with **CISA** and the **Department of Homeland Security** (DHS) to run a **simulated phishing attack** on **600** of their **1500 associates** who use computers for their daily workflow.*
>
> **Bill F. -** Director of Technology & Governance

> *We were floored by the results, and so was **CISA** and the **Department of Homeland Security.** The fact that only **1** in **600 took the bait was extraordinary.** After that, I think we all rest easier, knowing our employees have a **true security mindset**—all of this based on **actual results.** Thanks to **NINJIO** for reinforcing our **security-first culture** through current and relevant topics.*
>
> **Bill F. -** Director of Technology & Governance

## RESULTS

As part of this program, a simulated phishing attack—purportedly originating from the I.T. department and designed collaboratively by DHS and the organization—was launched to a randomly selected 600 employees as potential targets. It was an extensively thought out and well-crafted phishing attack, and both the organization and the DHS were shocked that only **one of 600 employees (or .17%) took the bait, beating the average by 18x*.**

In three years, shifted organization to a “security aware culture”.

Employees engage with and buy into the NINJIO content, creating a Cybersecurity “Identity”.

When faced with a simulated phishing attack, only .17% of employees took the bait.

According to the KnowBe4 **2018 Phishing By Industry Benchmarking Report**, after 12 months of computer based training, the average 1000+ company click rate was 3.04%. In this case, NINJIO beat that by 18x.