How Bit Sentinel helped increase phishing awareness for a major retail player in Romania

Industry: retail

Location: Romania

Employees: 4000+

Project started in: 2022

BIT SENTINEL

The Client_

_The client that opted for the Phish Enterprise services is one of the most important players in the Romanian retail sector.

_The company has over 4,000 employees in Romania.

The Challenge_

_The most effective cyber attacks require minimal technical resources precisely because they rely more on human error rather than on the lack of cutting-edge cybersecurity solutions in companies. Under strong pressure, people are more prone to making mistakes, which is the main reason why most data and security breaches succeed.

_In the market our client operates, there have been a series of phishing incidents that have caused devastating data and security breaches. The consequences were severe, with retail businesses suffering significant financial losses, reputational damage, and an erosion of customer trust.

_Our client understood that investing in training their human resource is likely the best and most efficient investment they can make for their cybersecurity defenses.

_To raise cybersecurity awareness throughout their network, our retail client chose to implement Phish Enterprise as an automated platform used for practical training exercises focused on cyber security and social engineering tactics that helps organisations develop their cyber culture and achieve compliance.

_As some of the company activities fall within the scope of the Network and Information Systems Directive (NIS), that imposes technical and organisational measures that cover, among others, user awareness and training while ensuring personnel security, Phish Enterprise has proven to be exceptionally well-suited to meet our client's needs in this regard.

The Solution_

_Our client opted for the "Auto-Pilot" version of Phish Enterprise to train their employees

_In this version, the team can use the entire set of 50+ available phishing attacks as a set-and-forget model, schedule scenarios and track results as a managed service. That way there was no need for the company to spend extra time and internal resources to efficiently reach their cybersecurity awareness goals.

The Methodology_

_For their internal cybersecurity awareness campaign, our retail client established the following training and testing strategy using the Phish Enterprise platform:

1. 1 to 3 weeks of studying the basics of
   - Phishing, Spear Phishing, Whaling, Smishing, Vishing
   - Malware, Ransomware
   - Computer viruses
   - Password security and management

   » the studying phase is then followed by an exam with questions from the above mentioned topics - all employees must pass

2. drafting a plan to launch phishing campaigns simulations that test the knowledge acquired in the theoretical part of the training; the phishing simulations should take into consideration the company's internal processes, technologies used for document sharing and the tools used by all company's departments (e.g. marketing, HR, admin, sales, procurement etc.)

3. rolling out the established phishing campaigns in the timeframe and for the teams approved by our client; the phishing scenarios varied, from messages appearing to be sent by widely-used platforms (e.g., Microsoft SharePoint, Google Drive, Office 365) to messages simulating internal processes (receiving CVs, proposal requests, invoice from suppliers, requests for password resets)

4. the Bit Sentinel team collects and analyzes data, provides analysis reports, and proposes improvement recommendations.

BIT SENTINEL

The Closure_

_After following every step of the cybersecurity awareness campaign and conducting the simulations provided through Phish Enterprise, our client registered the following results:

- **more vigilant employees, already expecting similar campaigns, which means they get more careful when it comes to malicious messages coming from unknown sources**
- **more engaged employees, willing to talk and share information about such campaigns, hence increasing cyber resilience within teams**
- **the rate of employee vulnerability to phishing attempts decreased by up to 80%**

Going the extra mile_

_After implementing the initial training and testing strategy using the Phish Enterprise platform, our client has agreed to continue working with the team at Bit Sentinel on the following projects that ensure a better cybersecurity posture for their company:

- Monthly testing conducted with quarterly reevaluation
- The client seeks increasingly intricate scenarios, involving the deployment of simulated ransomware attacks, malware infections, or pages seemingly requesting authentication credentials
- As a testament to their satisfaction, our client continues to engage our services and has expanded their collaboration to encompass other offerings such as SOC (Security Operations Center) and Pentest (Penetration Testing)

BIT SENTINEL

About Us_

BSS-CERT Security Operations Center_

One of the very first professional SOC-as-a-Service available for customers who need comprehensive detection, response, and threat intelligence capabilities.

Security Code Review_

Take an important step in the company SDLC and save time and money otherwise spent on fixes.

Penetration Testing_

We assist companies to interpret and act on threat data to ensure business continuity.

Managed Services_

We assess security controls and implement measures to ensure your setup stays resilient and compliant.

Security Compliance_

Get professional help to meet security prerequisites related to NIS, GDPR, PCI DSS.

Cybersecurity Awareness_

We help you promote a culture of security awareness throughout your company and beyond.

Social Engineering Campaigns_

We simulate social engineering attacks to uncover how vulnerable your employees are and educate them to identify attacks.

ONE-STOP-SHOP FOR CYBERSECURITY SERVICES

Let's have a talk!

Contact info_

Bit Sentinel

contact@bit-sentinel.com

bit-sentinel.com

BIT SENTINEL