# CASE STUDY

## Prison Commissary Cybersecurity

## Incident Timeline

1. **Initial Compromise:** The commissary fell victim to a phishing email containing a fake invoice, resulting in a payment of $10,000 via check.
2. **Second Attack Attempt:** Three months later, a second phishing email arrived, this time with a fraudulent invoice requesting a wire transfer of $250,000. Although the payment was approved, the bank's delay in processing allowed for a closer examination, revealing the invoice's fraudulent nature just in time to prevent the transfer.

## About the Customer

The prison commissary, a crucial lifeline for inmates to purchase essential goods, found itself under a cyber-attack that threatened its operations and security. This case study outlines the sequence of events, compromises made, and subsequent actions taken to enhance the commissary's cybersecurity posture.

## Investigation and Discovery

Upon discovering the attempted fraudulent transfer, the commissary sought assistance to investigate the incident. It was uncovered that the second invoice contained a malicious payload, granting the attacker access to the internal network. This network interconnected with VPN connections to 150 jails and prisons, amplifying the potential impact of the breach significantly.

## Remediation Efforts

Promptly after the discovery, a comprehensive plan for eradication and remediation was set in motion. The focus was not only on removing the malicious elements but also on strengthening the commissary's overall security posture to prevent future incidents.

Telesystem
IT's About Trust

## Recommendations Implemented

1. **Security Awareness Training:** Educating staff about phishing emails and other social engineering tactics to recognize and report suspicious activities.
2. **Vulnerability Management:** Regular assessment and patching of vulnerabilities within the network infrastructure and software systems.
3. **Endpoint Detection and Response (EDR/XDR):** Deploying advanced endpoint security solutions to detect and respond to threats effectively.
4. **Payment Processing Separation of Duties:** Implementing stricter controls and segregation of duties to prevent unauthorized payments.
5. **Incident Response Planning and Training:** Developing and practicing incident response plans to efficiently handle future security incidents.
6. **Updated and Managed Next-Generation Firewalls (NGFWs):** Enhancing network perimeter security with modern firewall solutions to better defend against cyber threats.

## Outcome

By diligently implementing the recommended security measures, the prison commissary significantly improved its cybersecurity maturity. The combination of enhanced awareness, fortified defenses, and structured incident response capabilities fortified the organization against potential future attacks.

## Conclusion

The cyber-attack on the prison commissary served as a wake-up call, highlighting the critical importance of cybersecurity in safeguarding essential services. Through collaboration with cybersecurity experts and the diligent implementation of recommended measures, the commissary emerged stronger and more resilient, ready to face future challenges with confidence.