LORICCA

Managed Security Services

PHISHING CASE STUDY

Phishing attacks are on the rise. With a strong security program in place, you can identify, protect, detect, respond and recover quickly.

About The Breach

In early 2022, a national non-profit became the victim of a whaling attack that targets high-profile employees, such as a chief executive officer or a chief financial officer, to steal sensitive information from a company. Scammers are often updating their tactics, and at first glance, the email or text received looks real, but it’s not.

In this case study, the attackers sent the victim an email that appeared to be from a trusted source. The attackers included a link to a customized malicious website and asked the victim to enter user credentials that had been created specifically for the attack. This allowed the attacker to access the victim’s email account, which led to stealing highly sensitive information.

What are the Consequences?

Due to the data that was compromised, the company was required to report and manage the incident. The reporting had to be compliant with all federal, state, and other regulatory authorities.

Financial loss due to remediation totaled approximately $1 million. Costs included evidence gathering, notifications to customers, security consulting fees, and the implementation of new security solutions.

In addition to financial loss, the non-profit’s cyber insurance carrier had decreased coverage because of the security weakness that contributed to the breach.

What is the Solution?

Email and web filters can identify and block many phishing emails and malicious websites, but without extra layers of protection, this non-profit was vulnerable to the attack. Keeping organizations secure requires effective procedures to identify, protect, detect, respond, and recover from security incidents. These tools include technical solutions, policies, training, monitoring systems, and regular updating of the information systems.

The non-profit engaged with Loricca to assist in the data collection and remediation strategy necessary to comply with state and federal regulations. A Security Risk Assessment was performed to identify gaps and build out a security program. The customer, in conjunction with Loricca, worked on remediating the identified security gaps found during the assessment.

The program involved writing custom policies and supporting the review and implementation of each policy. Loricca also replaced end-of-life systems that were in the non-profit's data center and deployed a new incident response plan which included training needed to manage the plan. Additionally, Loricca supported the non-profit with:

- Risk management processes.
- Migration of existing infrastructure to Azure.
- Multifactor authentication.
- Incident response planning.
- Vulnerability management.
- Security awareness training.
- Data management.
- Event monitoring (SIEM).
- System development lifecycle.
- Supplier risk management.
- Updated security policies and procedures.

Lessons Learned

Preventing cybercrime requires a multi-layer security approach to address the tools, technology and people. Additionally, effective procedures to identify, detect, protect, respond and recover from security incidents are critical to keeping organizations secure.

Functioning as the non-profit’s Chief Information Security Officer (CISO) and working with their leadership team, Loricca helped integrate additional security measures into their daily activities.

After providing supporting documentation of the remediation and security program, the cyber insurance carrier restored full coverage.

Loricca continues to partner with the non-profit’s IT team as their virtual CISO to provide ongoing support.

FOR HELP PROTECTING YOUR INFRASTRUCTURE AND COMPANY, CONTACT US. www.loricca.com | 855-447-2210

ABOUT LORICCA

Loricca provides world-class consulting services required to meet today’s cybersecurity challenges. Our security professionals bring a wealth of experience with real-life lessons on what works and what doesn’t.

We partner with organizations to evaluate, build, and manage their IT security programs. Our experience spans across many industries including healthcare, government, media, retail, finance, software, and medical device manufacturing.
Our goal is to keep these organizations and their vendors compliant and protected from the cybersecurity risks of today and tomorrow by delivering high-quality work on time and on budget.