Security Awareness Training Case Study

J. Embree

Department of Cybersecurity, SNHU

CYB 200: Cybersecurity Foundations

April 13, 2025

Security Awareness Training Case Study

Phishing

Phishing is a prevalent fraud tactic, used by attackers to "trick the victim into providing private information." (Kim and Solomon, 2023, p. 516). The consequences of phishing include financial losses, data breaches, reputational damage, operational disruption, regulatory and legal consequences, and loss of competitive advantage. (Parker, n. d.).

In Fizza Cola's case, the phishing attack emails led to malware installation on company computers and required new hardware. The highest concern is that phishing will lead to theft of credentials (for access to accounts) and intellectual property (including trade secrets and copyrights). These attacks bring to light that the company is not following the NIST cybersecurity framework: identify, protect, detect, respond, and recover. (N.I.S.T., 2024). The failures occurred during the identify, protect, and detect stages.

Human Factors

By some estimates, 90% of cyber breaches are caused by human errors and phishing is one of the top attack types. (Glen, 2025). Fizza Cola's initial phishing incident that led to the malware installation most likely occurred when untrained employees clicked on email links. These employees may have been locked out of their accounts and unable to perform their duties. The situation would have been embarrassing and frustrating to the employees as well, once they discovered they had been tricked by illegitimate emails.

Not only did Fizza Cola have extra costs from purchasing new hardware, but implementing training and security software will also add to company expenditure. If Fizza Cola's intellectual property had been stolen, there would be massive costs to rebuild the brand,

copyrighted material, and trade secrets. It could also harm the company if customer trust in Fizza Cola was damaged by fraudulent copies.

If the phishing attack's malware had installed ransomware, the company would have had to make a choice to lose valuable data or pay a ransom for the encryption key from the hacker. Fortunately, it seems like these phishing attacks did not cause catastrophic damage so they can be viewed as an opportunity to improve security and implement better protocols into awareness training.

Legal Factors

Besides consequences like disrupting business and losing confidential data, security breaches can lead to the following (Pittman et al, 2023):

- Heavy fines or regulatory sanctions,
- Government audits and investigations,
- Loss of market position and even lawsuits from the shareholders as a result,
- Negative media attention,
- Loss of consumer trust and potential litigation from customers, and
- Lawsuits from employees (for the lack of proper training).

The legal impacts of breaches should be incorporated into Fizza Cola's security awareness program, to ensure employees understand the far-reaching effects of phishing or other attacks.

Benefits of a Proactive Security Mindset

Because the whole company should function as a team, it is important for all employees and all levels of the organization to be in agreement when it comes to security. All employees need to understand how to identify and properly respond to threats, to avoid future breaches. Company leadership needs to understand the importance of training, and how it saves costs by preventing breaches.

Recommendations

Fizza Cola needs to have a security program to prevent future security breaches, including:

- Mandatory training for all employees.
- The frequency of training meetings should be at least every 4-6 months, for better retention. (Reinheimer et al, 2020).
- The meetings should be kept to a maximum of 30 minutes and include time for employees to ask questions and contribute to the discussion. The goal of the meetings is to cover policy (or updates), briefly discuss security risks, and encourage feedback from the employees.
- Once a month, employees should be sent a reminder email that has screenshot examples of phishing. It might help to use short, interactive training modules or games that employees can go through at their own pace.
- Employees should be encouraged to notify their supervisor of suspicious emails before deleting, reporting, and blocking the sender.

- Any incident that occurs should be used as a learning opportunity, to improve training and promote awareness.
- Regular surveys should be conducted (every 3 months) to ascertain employee awareness and the effectiveness of the training.

A few other steps Fizza Cola should take to avoid phishing attacks include (Parker, n. d.):

- Utilizing security tools to detect, filter, and block suspicious emails.
- Using multi-factor authentication (MFA) to protect accounts and systems.
- Creating and regularly testing an incident response plan to decrease the effect of future attacks.
    - This could be incorporated into a disaster recovery plan, and part of the business continuity plan (BCP). (Kim and Solomon, 2023, p. 371).

References

Gren, Christy. (March 11, 2025). *Cybersecurity Breach: How Human Errors Lead to Most Risks?* Industry Leaders. https://www.industryleadersmagazine.com/cybersecurity-breach-how-human-errors-lead-to-most-risks/

Kim, David and Solomon, Michael G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones & Bartlett Learning.

National Institute of Standards and Technology. (February 26, 2024). *The CSF 1.1 Five Functions*. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

Parker, James. (n. d.). *How Does Phishing Impact Businesses and Organisations?* Cyberly. https://www.cyberly.org/en/how-does-phishing-impact-businesses-and-organisations/index.html

Pittman, F. Paul, et al. (March 22, 2023). *Cybersecurity Developments and Legal Issues*. White & Case. https://www.whitecase.com/insight-alert/cybersecurity-developments-and-legal-issues

Reinheimer, Benjamin, et al. (2020). *An Investigation of Phishing Awareness and Education Over Time: When and How to Best Remind Users*. Usenix. https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf