Security Awareness Training Case Study

William Pascoe

CYB-200: Cybersecurity Foundations

Robert Brickan

August 9, 2025

Security Awareness Training Case Study

Recently our company, Fizza Cola, has been getting several emails that were in fact phishing emails and resulted in malware being installed on workstations. A phishing email is a type of social engineering security risk wherein the sender makes it appear that the email is legitimate like “look at this report” or “You won a dream vacation”. When an unsuspecting person opens this email and clicks on the link they may not notice anything happen but in the background the email opened a program that installed some sort of malware onto that workstation. This malware can be a virus that retrieves and sends information somewhere or installs what is known as a backdoor and allows a hacker to gain access to the network during times when people are not around and notice something happening. As a result of these events the company has invested in new technology to help detect and eliminate the threats. Now we are going to look at some ways in which we can expand our training program to help personnel identify and deal with these threats.

Human Factors

When it comes to cybersecurity the weakest link in the chain is human errors and they can be hard to mitigate (Kost, 2024). All humans make mistakes and if we aren’t careful those mistakes can be costly. The only way that we can help reduce those mistakes is through training. If we teach and show people what a phishing email is, what to do when you suspect one and maybe even test them in a controlled environment, then we can reduce the threat to a minimum. If we don’t develop such a program, then we will continue to have more phishing attacks and as it goes on threat actors will get smarter and make their attacks more sophisticated and could do more harm and damage to the company. The worst harm that a company can have thrown upon them is their reputation. If this company is known to always have attacks against it people and

other businesses will not want to have dealings with us because they will not trust their personal data to us.

Legal Factors

Businesses also have a legal obligation to keep their data secure. We need to ensure that policies and guidance are easy to understand and readily available for all staff (Deighton, 2015). If we don't, a breach can cause a loss in trade secrets, personal data or even financial losses both from the hackers or from fines related to government regulations. Policies will not assist in defending a fine if staff never refers to them or has difficulty understanding their practical application (Deighton, 2015). Staff should be trained not only trained on how to recognize an attempted breach but also understand why we don't want that breach to happen.

Proactive security mindset

Having a proactive security mindset means that you are always making sure that everything remains secure. Whether it is ensuring no one is tailgating you into the building or making sure your workstation is locked when going on break or getting a cup of coffee. You always want to be aware of your surroundings and think that whatever you do could have potential security impacts on the company. This must come from all levels of the company. An important cybersecurity principle here that comes to mind is zero trust. Whether someone is the CEO or an intern, we never give them more access to information than they need to do their job. If we operate on that principle we keep the data of the company, its employees and its customer as safe as we can. We also must make sure that through training we keep everyone aware of what can happen if we are not careful and set them for success.

References:

Kost, E. (2024). *Human Factors in Cybersecurity in 2024 | UpGuard*. Upguard.com. https://www.upguard.com/blog/human-factors-in-cybersecurity

Deighton, A (2015). *Cyber security: the dos, the don'ts and the legal issues you need to understand*. (2015). Financier Worldwide. https://www.financierworldwide.com/cyber-security-the-dos-the-donts-and-the-legal-issues-you-need-to-understand