Week 1 Assignment: Training and Educating Users

Shaun Hoadley

CST316: Information Security Management

Professor Amr Elchouemi

July 12, 2021

**Types of training for mitigating social engineering.**

There are a lot of ways to train to mitigate social engineering. There are scores of videos commercially available as well as free on video hosting sites like YouTube. For the latter, TEDTalks are particularly informative from my experience. One TEDx video I enjoyed was by Brian Bushwood and his “school of scam” (2011). Another effective training method is to have training meetings where the participants roleplay scenarios of social engineering techniques. There are classes at colleges and universities, particularly in the fields of psychology, that go into depth on social engineering. While not advertised as such, marketing courses teach social engineering techniques to make one more effective at marketing; after all, the goal is to convince others to purchase the products or services.

**Administrative tools to track and mitigate social engineering**

There are many tools at one’s disposal to track and fight social engineering. Whether in a physical or digital environment, the first tool one can use against social engineering is authentication logs. This could be an entry log by security or receptionist in a physical environment, or it could be a user log generated after someone accesses a computer or network system using authentication credentials. An often overlooked tool to defend against social engineering is the spam settings for email clients. The spam settings are, in many cases, adjustable using various filters to identify, filter out, and mark as suspicious emails that may be used maliciously. Password vaults are helpful for generating and securely storing passwords for one’s accounts. One should always use different passwords for each account they access; otherwise, if someone gets the password for one account, they can access all of the accounts using the same password.

**Data Integrity**

According to Wills, “Integrity, in the most common sense of the word, means that something is whole and complete, and that its parts are smoothly joined together.” (2019, p. 30). Data integrity is essentially the health and maintenance of data throughout its lifecycle. This means that maintaining the validity and accuracy of data ensures that the data is connectable, recoverable, searchable, and traceable to its origin. It is, therefore, vital that employees have knowledge of data integrity and good practices for keeping data integrity intact. Not maintaining data integrity could have severe costs, such as losing clients by not having the data needed on hand or giving them the wrong information based on inaccurate or even obsolete data.

**References**

TEDxSanAntonio. (2011, December 11). *Brian Brushwood - Social Engineering - How to Scam Your Way into Anything*  [video]. YouTube. <https://www.youtube.com/watch?v=yY-lMkeZVuY>

Wills, M. (2019). [(ISC)2 SSCP Systems security certified practitioner: Official study guide](https://ashford.instructure.com/courses/87741/modules/items/4439845) (2nd ed.). John Wiley & Sons.