SEng 360 - Assignment 2

Name: Kenil Shah

V00903842

Summary

The aim of this social engineering attack is to get access to the user's phone, particularly their ride sharing account to mainly track and monitor the location of a particular target as destination and route are already decided prior to target even entering the car. This will be accomplished by launching a spear phishing attack on the user. The target will be sent an email or a text message warning them that there was an information breach on the server end and there is a chance that their data might have been stolen. It will be heavily implied that the data stolen is highly sensitive, but as a solution to the problem a link will be presented as a simple one step solution. The aim of getting access to the account is to have access to personal information such as phone number, name, home address, credit card information, and most importantly route information. The email or text message will contain a link to a fake website where they will enter their name, email address/username attached to the account and their password.

The mitigation to this approach is to force the users to apply 2 factor authentication to their account. This will add a layer of protection in case where the attacker gets hold of username and passwords

Psychological principles

The scenario initially presented about a data breach is quite topical and is more likely to catch people’s attention. This scenario is more likely to aggravate a target's emotions as it has become a common place in this day and age. In addition, the fact that there might be potentially sensitive and personal information that was leaked, and implying that this will cause serious personal harm will add on a sense of urgency and help tunnel the victim to go forward with the only available mitigation at this time. The link provided with email acts as an easy, simple and at this time a seemingly logical solution, as the target would be tunneled at this point. Combined this will lead the target to fall into the trap.

Mitigations

Some basic mitigation tactics are as follows:

First is to introduce and force users to apply two factor authorization on their accounts. This is to help in case their credentials to the account do get leaked, the attacker still would not gain access to the accounts just on that basis.

Second is to educate and warn the user to not enter their credentials outside the app. This warning can also be implemented to show up at regular intervals when the user is using the app.

In case, there is a data breach this notification should be sent through the app; in the form of a push notification or in-app notification.