The Art of Hacking Humans: Intro to Social Engineering

Shoulder Surfing

Shoulder surfing involves a malicious attacker stealing confidential and sensitive data from unsuspecting victims essentially by looking over the victims shoulder. The main thing about shoulder surfing is that the attacker steals the data without the victim being aware, this can be achieved by peeping over the victim’s shoulder, using hidden cameras, installing keystroke loggers, ATM skimmers, and the like. An intruder could steal usernames, passwords or PIN codes which they can use to compromise their victims and take over their access, or steal data or funds. So shoulder surfing can be defined as a method of stealing confidential and sensitive data (like login credentials) by using a form of surveillance or the other (the surveillance could be peeping over shoulder, using hidden camera or skimmers and so on).

Criminals have been known to install hidden cameras at ATM points to steal card PINs as they are being entered. They also install fake keypads on ATMs used to collect card details, and ATM skimmers can be inserted in card slots and used to steal card data. Krebs on security (2013) gave an example of a skimmer found November 2013 in Brazil which was a complete fake ATM placed over the real one at a bank. The customers would insert their cards and enter PINs only to get apparent errors, not knowing that their card details and PINs have been compromised.

Shoulder surfing takes advantage of victims’ sense of security, inattentiveness and negligence. The victims usually feel they are in their comfort zones so nothing is likely to go wrong; hence their guard is down, giving the attacker an upper hand.

The menace of shoulder surfing can be tackled with alertness and extra vigilance. In office environments where there are cubicles that are not see-through, employees should avoid leaving their doors open (especially when entering login credentials on their computing endpoints). Institutions that maintain ATMs (like banks) should educate both their employees and customers on entering PINs discretely (covering with keypad with the other hand when entering the PIN is a good idea) such that someone behind cannot peep to see what was being typed. The organizations should also further educate both employees and customers on detecting surveillance devices like hidden cameras and also how to detect skimmers. Criminals tend to install skimmers and cameras during times when banks are closed for long periods and there is high ATM traffic, like weekends and holidays, and then take them off at the end of such periods (Krebs on security, 2013). Those periods not only have more likely victims using the machines, but also there is less likely to be personnel attending to the machines during the periods decreasing the chances of detection. Therefore, there should be further extra vigilance during such periods.

References:

Krebs on Security (2013) *The Biggest Skimmers of All: Fake ATMs* [Online]. Available from: https://krebsonsecurity.com/2013/12/the-biggest-skimmers-of-all-fake-atms/ (Accessed: 29 October, 2017).