Adrian N
an9905@rit.edu
CSEC.468.01
Risk Management for Information Security
Project Group – Social Engineering

Even though technology and humans are both depicted as risk vectors in cyber-physical systems, it is the human susceptibility to errors that is seen as the main problem in current cybersecurity discourses. In the paper, “Hacking Humans? Social Engineering and the Construction of the Deficient User in Cybersecurity discourses” it states, “risk is mainly seen as individual risk that increases with the number of employees. As this interviewee stated, it is now up to them to keep the network secure, as every employee must be as cautious and well trained in spotting suspicious activity as the guard at the gate (IP 1)”. This quote pretty much summarizes the focal point of the article in that a lot of social engineering is about ‘hacking’ humans. Computers cannot make mistakes as they cannot think for themselves, but we behind the computer contribute to 99% of the errors that lead to data breaches/hacks/attacks. The paper also speaks on how most of these workers are the office workers, accountants, and/or technicians. They are not used to being targeted, as they do not believe they are the ones susceptible to phishing emails or social engineering attacks in general, when in fact they are the main target. How are they supposed to know that there are attacks deliberately designed for them, while going about their regular business, unless they are educated. Therefore, it connects and applies to our project, as I was thinking that we can use this as an example to create a policy where every potential employee must do some training for social engineering. We would then test them throughout their tenure at the company to make sure they are up to date with the newest social engineering attacks. This paper in general applies to risk management as a huge part of risk management is to prepare for attacks, and to think like a hacker. Any framework includes the prepare phase and to assess controls and monitor them. The frameworks specify that the organization must understand every employee’s role, and give them appropriate access to certain things, and denying their access to other things. There is no reason an accountant should have access to a mainframe with all the businesses contact information etc. because a potential hacker will target the accountant, as they are a weak link and then get this information to then send deliberate specific phishing emails to get into another system. In all this paper had a pretty in-depth view of how social engineering works, in regards to who is targeted and why. It helps us understand how to mitigate these risks, and who to specifically watch out for / monitor if some social engineering attacks were to occur.

References

Nina Klimburg-Witjes, A. W. (2021, February 10). *Hacking humans? Social engineering and the construction of The "DEFICIENT user" in CYBERSECURITY Discourses - Nina KLIMBURG-WITJES, Alexander wentland, 2021*. SAGE Journals. Retrieved September 15, 2021, from https://journals.sagepub.com/doi/full/10.1177/0162243921992844.