Related work

The weakest point of a technological system is the people. The psychological manipulation of people in order to gain access to a system for which the attacker is not authorized is often easier than hacking into the hardened software system. And this is the problem we need to solve, a commonly used approach to solve this issue is to make them aware. Training-based training pushes employees to be aware of the consequences of each step they make in their communication. This type of training approaches relies on the human to prevent attacks manually. But this approach still has its vulnerabilities because the human has his vulnerability to social engineering, and it depends on the human’s emotional state of the time of attack.

People who receive that type of social engineering training is expected to have more self-disciplinary awareness by following specific steps to answer any answer from external sources, like “Is this answer confidential to our organization?”, “Should that person ask for this information? “, “Who should have the privilege to ask this question?”, by following these steps the employee should be able to control the communication with external agents. Maintaining to keep following these questions is often hard especially when the employee is under the emotional influence of the social engineer.

For automatic detection of suspicious emails there is a number o approaches to detect phishing emails using email headers, SMTP headers NIDS logs and others. What we are interested in is the approaches that are focused on processing email content or parts of it. One way of doing that is preforming authorship of identification, to analyze email features and assuring that who claimed to be the sender of the email in the content is really the sender. These approaches characterize emails by using statistics on frequency of words using n-grams. One example of that is ASCAI which generates a writeprint of senders, then generate another writeprint for the current email sender, and compare against the list of known senders’ writeprints to verify authorship.