As we are working for search for the best method to reveal how the attackers make their way through users’ sensitive data and information, We had to understand the scope of which they perform, in example trying to fetch important data through out phishing techniques using malware links made using penetration testing tools. Other way, hackers could send spammed emails, targeting huge number of users with different authorities in which they could lead to the wanted person or manager they need.

So in order to achieve this we have splitted the vast majority of attacks into two different categories. The first group is using **Ask a question** whose answer is private or leads to data breach. The second group is using **Issuing command** to perform a forbidden function. So we have made our way through that by diving attackers’ commands into a **verb-object pair** so that we can easily identify which commands could be a threaten to users’ sensitive information.

In the phase of question analysis, we commonly see a pattern that the user is prompted to enter data in shape of form questions which could be parsed into a form that is really spread in usage. After a lot of research the way is to ask the victim about his important or sensitive data. It is not directly from about the content but it just the start to lure the victim to answer it even more sensitive data. The way we are going to deal with it would be to divide the question in example of "wh" questions looking for item wanted in the question (e. g.) "what is your <item>?" where "item" mentioned is the form item (data).