One of the most popular attacks is phishing attacks, which ask for a reaction from the victim.

The attacker is being disguised as popular website banks,

administrators from IT departments. It starts sending emails in perfect format to the victim.

These emails lead the user to interact by clicking and then this device starts to download malware or open a form that he has to fill in with his personal information.

In previous research related to phishing email detection, such as the phishing website filters built into Microsoft Internet Explorer and Mozilla Firefox.

Another related previous work was training individuals on social engineering attacks in order to make them more aware and resistant in the future, and this is considered more effective as individuals are always the weakest layer in the system, but it costs more time and effort.

There is another type of attack that is no less dangerous than phishing attacks: it's not depending on emails but includes calls and texting, and in-person communication.

Email communication is not real-time, Email communication is not real-time, the attacker doesn't expect he will receive the response immediately, or may the attacker never respond.

But the non-email way being in a real-time involved two-way conversation.

The conversation is better for the attacker because it pressures the target to respond without spending time considering the consequences, and that's made from the known-email attacks more efficient.

Existing methods for automatically detecting social engineering attempts are primarily focused on phishing emails.

These methods rely primarily on non-content metadata present in emails, such as contained hyperlinks and SMTP headers, for analysis.

Non-email social engineering assaults that aren't associated with accessible information aren't detected by these techniques. When you don't have any metadata to rely on.

There are content-based techniques that look at things like character frequency and word/n-gram frequency in the material.

These methods, on the other hand, do not use semantic analysis to extract the meaning of the text and the attacker's aim. The application of existing content-based metrics alone, without semantic analysis, would result in low precision and accuracy.