

Abstract

- Social engineering has become a nuisance to UK businesses and the wider economy, as these attacks drain resources from Information Technology (IT) departments. Organisations are constantly fighting a losing battle to protect their assets from hackers and keep hold of the perception of good cyber security.

- This project included a qualitative literature review analysing social engineering methods, attack vectors, attack channels and other aspects of social engineering that will also support the methods used in the experiment. The project also includes a quantitative field experiment, which the results will be analysed and compared with literature to create mitigation strategies a company could implement.

- Social engineering attacks are difficult to defend and damaging to an organisation. In the experiment, the methods used for physical social engineering attacks were successful. They required little technical expertise but did require confidence and understanding of the way in

Background

Social engineering (SE) attacks are attempts by an attacker to convince people to reveal sensitive information, without alerting them of dishonest activity.

Common SE Attack Methods:

- Phishing

Phishing is usually malicious emails sent on mass that attempt to convince a victim to click a link and give some kind of personal or confidential data [1].

- Spear phishing

Spear phishing is a more direct phishing attack, often only focusing on an individual or small group as the attack is tailored with specific information that has likely been collected via other means [2].

- Vishing

Vishing or voice phishing is a variation of phishing where an attacker uses a voice call to collect the same data a phishing email is after [3].

- Smishing

Smishing or SMS phishing is also a variation of phishing where an attacker uses text messages with compromised links to fake sites, in an attempt to harvest credentials or personal information [3].

- Whaling

Whaling is a similar attack as spear phishing, where the target is a specific individual. However, with a whaling attack, the victim is a person of significant authority in an organisation i.e., a CEO, CFO, IT Director, or HR Director [4].

- Dumpster Diving

This attack requires the attacker to go through rubbish bins and other waste containers to find valuable information that a person or business may have thrown away, not knowing the significance of the information [4].

- Shoulder Surfing

Shoulder surfing is another physical attack where an attacker (this could be anyone who should not see the content on the screen or desk of the victim) hovers discreetly around a victim's workstation and attempts to read and digest information that's laying around or left on screen [4].

- Baiting

An attacker loads a storage medium with malicious software, to then leave it laying around

Hypothesis and Objectives

"Social engineering attacks can be mitigated through a combination of technical solutions, security awareness training, and strong policies and procedures."

Social engineering attacks rely on manipulating human behaviour to gain unauthorised access or information. Technical solutions such as firewalls, antivirus software, and intrusion detection systems can help detect and prevent these attacks, but they are not fool proof [1]

The planned objectives:

- Investigate the organisation for any information that could prove useful for each of the planned SE attacks.
- Prepare the attacks using the information gathered. For example, create the phishing sites, host the phishing sites, etc.

- Execute the deception phase. This would be when the method is sent to the user.

- Visit the site after the investigation phase of the physical SE attack vectors.

- Analyse the results and determine if they were a success and if they could continue to the next lifecycle phase.

The social engineering life cycle follows these phases, Investigation, Deception, Attack, Exit.



Figure 2 - The social engineering life cycle

Technical Attacks

In the project, there was an attempt at the following technical attacks. Here are the outcomes:

Experiment 1 & 2: Phishing & Spear Phishing - This experiment was ultimately unsuccessful and required further technical understanding of business email security. However, the preparation/investigation section of these attacks did however find that a few directors were too forthcoming with information available on their social media accounts.

Experiment 3 – Whaling - This experiment was partially successful, the target was one of the directors who had their mobile number listed on LinkedIn. With the information available to me, I Smishing attack was possible and some location and device data was collected.

Experiment 4 – Baiting - This experiment was also a partial success. 10 USB devices were scattered around the campus. These devices were mostly returned to the IT director, however, 7 clicks on the compromised files were recorded and a few device and operating

Conclusion & Further Research

Social engineering attacks are difficult to defend and damaging to an organisation. There is no perfect mitigation however, staff training and strong policies and procedures are some of the best mitigation strategies. One of the best defences would be to raise awareness and understanding of social engineering, keeping it at the forefront of the employees' mind, with regular updates and training. Further Research into the effects of AI the defence against SE attacks, this could benefit smaller organisations who are already struggling to find/ afford cybersecurity experts. Research cross-cultural differences in social engineering tactics and how the could be adapted to other areas.

Physical attacks

In the project, there was an attempt at the following physical attack. Here is the outcome:

Experiment 5 – Piggybacking / Pretexting / Shoulder Surfing

In this experiment, I successfully penetrated the organisation using the physical social engineering methods above.

Having the confidence, a prepared look, background story and prior information gathered is key to the success of these attacks. The professional look was praised by the director of IT stating that "I knew you were coming but I still felt I did not know you or feel like you did not belong". The combination of these factors allowed the attacks to be so successful. The moment that hesitation was shown, people got suspicious.

The conclusion drawn from these scenarios suggested that unsuspecting people are vulnerable to SE attack. This gave great insight into the world of physical social engineering

Mitigations

After conducting research and running the experiments. These are the recommended mitigations:

- Remove unnecessary contact information from social media sites and uses shared mailboxes where possible. i.e., info@copanya.com, sales@companya.com. This will make it more difficult to find personal information.

- Always stay alert when receiving SMS messages. Do not trust every message you receive. Do not click links, even those from trusted contacts, unless you confirm its content.

- Regular test phishing campaigns. The organisation could utilise built in tools in the Office 365 environment to send and track phishing emails internally. This would help track internal contacts who fall for these attacks and offer further training and guidance.

- Routine cyber security training should be carried out.

- Policy changes should be implemented, to make users more accountable and responsible of security.

- Consideration should be made that USB ports should be disabled and only to be available for mouse and keyboards.

- Employees should be required to wear an identification badge or lanyard to show they are authorised to be in that area.

- All visitors should be escorted to and from the arears of work.

- implement a 'clear desk policy'. This means that the owner of the desk space must keep their work area clear when they are not present at the desk

References

- [1] - A. Alharbi, A. Alotaibi, L. Alghofaili, M. Alsalamah, N. Alwasil and S. Elkhediri, "Security in Social-Media: Awareness of Phishing Attacks Techniques and Countermeasures," in 2022 2nd International Conference on Computing and Information Technology (ICCIIT), Tabuk, Saudi Arabia, 2022.
- [2] - Barracuda, "Spear Phishing: Top Threats and Trends," Barracuda, 2021.
- [3] - J. H. a. C. M. Laurie Iacono, "The Rise of Vishing and Smishing Attacks – The Monitor, Issue 21," Kroll, 02 09 2022. [Online].
- [4] - O. Ş. A. I. C. Valerică GREAVU-ŞERBAN, "Social Engineering a General Approach," Informatica Economică, vol. 18, no. 2, 2014.

