Introsec-Assignment2

Task 5 Social Engineering

Students Names: Ahmed Al-Ghadhban, Mohammed Raiyan

Introduction

Social engineering in the domain of information security is defined as the malicious act of deceiving humans(victims) into giving access to their personal information, secrets, or sensitive information to the attacker (social engineer or hacker) [1], social engineering attacks uses a combination of techniques to form the attack, some examples of techniques can be phishing, pretexting, baiting and more.[2]

The attacks can be direct attacks where the attacker communicates directly with the attacker and this communication can be one directional or two directional communications, the attacks can also be indirect through a 3rd party source like a webpage, E-mail, SMS and more. [2]

In this assignment we interviewed 6 participants after identifying and designing 2 real-life scenarios where social engineering can be used to breach IT security policies, for each of these 2 scenarios we interviewed 3 individuals, the aim of this experiment is to assess the public's awareness of social engineering risks, understand how serious the threats in specific scenarios are, assess people's views on potential damage, and evaluate how well current security measures handle these risks.

Design

a. **Scenario 1**

   In this scenario, the attacker set up a fake public Wi-Fi hotspot with a name that resembles a legitimate network in popular areas of Stockholm, such as university libraries, cafes, or hotels. Unsuspecting individuals connect to these fake networks, allowing the attackers to intercept and potentially manipulate their internet traffic.

In this scenario, the attacker will manipulate his victims into thinking that they are accessing a legitimate public Wi-Fi network but instead they are connecting to the attacker's unencrypted Wi-Fi network, this type of attack is known "evil twins" attacks, when the victim access such networks, when performed flawlessly, victims will be vulnerable to a long list of information security threats such as stealing personal/sensitive information, stealing log in credentials, stealing bank log in credentials, inserting a malware and more.[3]

b. **Scenario 2**

   In this scenario, an attacker sends a deceptive email to the victims (students in our scenario) posing as the student accommodation, the E-mail looks identical to that they usually receive from the trusted accommodation and with an attachment for the monthly rental invoice, without checking the checking the source the student opens the attachment.

In this scenario, the attacker manipulates his victims into thinking they received a legitimate email that resembles the title and look of an email they usually receive from the trusted source and click on attachment or a link, this type of attack can leave the victim vulnerable to a list of information security attacks that can lead to installing malwares that can steal sensitive information, ransomware where the

attacker encrypt the victims data and demand to be paid in-order to give back the access to such data, implement keyloggers through the attachment to steal credentials, and more different types of attacks.[4]

Interview findings

1-Scenario 1

- *Using public Wi-Fi*

All 3 participants frequently access and use public Wi-Fis in cafés, libraries, and trains at least 3 times a week as one participant stated and every day as another participant said, and the reasoning behind using public Wi-Fi for all 3 participants was mainly to save mobile data.

-Awareness of potential risks

When asked about if they are aware of the potential risk of accessing public Wi-Fis, one participant said that she have an idea but lacks specific details of such risks, another participant seemed less concerned about such threats and admitted to accessing open Wi-fi networks without much concern, but the 3rd participant said that he is fully aware of the risks and that he read about them previously.

-Security measures

When asked about the security measures they take when accessing public Wi-fi, all 3 participants said that they try to use it mainly for browsing, avoid accessing portals with sensitive credentials and avoid online banking and online purchasing when on public Wi-fi, although all 3 of them admitted to using online banking or bankID on a public Wi-fi before, one participant mentioned that he " turns off network sharing options and enable firewall" when accessing a public Wi-Fi. Another participant mentioned that he only accesses trusted services and websites when on public Wi-Fi.

-Knowledge of VPNs

The participants seemed familiar with the concept of VPNs but are unaware of the importance of VPNs when accessing public Wi-Fis and rarely use VPNs, they only use it when the there is a restriction to accessing certain online services through public Wi-Fi.

-Potential victims to our scenario

All 3 participants admitted that they can fall victims to our scenario if such an attack is orchestrated flawlessly.

2-Scenario 2

-Receiving fraudulent emails

All 3 Participants stated that nowadays they rarely receive fraudulent emails in their inbox, but their spam folder usually receive such emails, but they tend to ignore and not open spam emails, though they agreed that couple of years ago they used to receive fraudulent emails more often than now even in their focused inboxes.

-Past encounters with fraudulent emails

one participant stated that one time she clicked on a link provided by an email that looked legitimate that caused her to lose access to her social media account but managed to recover the account later, another participant many years ago he felt victim to an attack where he clicked on a link provided by an email that

led a virus attack on his machine that forced him format his computer, the last participant had no encounters where he fell victim to malicious emails.

- *Awareness of potential risks*

All 3 participants seemed to be aware of the potential security risks of downloading an attachment or opening a link from a suspected email.2 participants relate their awareness to previous encounters which forced them to read about potential risks and attacks when opening an email links or attachment.

-*Security Measures*

All 3 participants said that they rarely open an attachment or a link they receive on their emails without checking and verifying the email sender address, one participant said that he never opens a suspected email at all and reports and delete such emails.

-*Potential victims to our scenario*

All 3 participants seemed confident in identifying such possible attack, and that they always check and validate the sender email before opening such attachment, but one individual said that anything is possible and that it will depend on the moment that he opens the email if he is occupied by something else, he might rush into it and opens the mail before checking.

Discussion

The number of participants for each scenario doesn't allow us to generalize or come to specific conclusions as this is the main limitation of this experience but it does give us an insight into the public awareness of social engineering in the domain of information security, and the potential success of such hypothetical scenarios from a limited sample size.

Scenario 1public Wi-fi twin attack

Generally, the participants showed a decent level of awareness regarding the risks associated with public Wi-Fi usage. But the Familiarity with potential dangers varied, with some acknowledging the risks while others were less informed. The participants mainly exhibited caution when accessing sensitive tasks that requires sensitive information like mobile banking and online purchasing when using the public Wi-fi and try to limit their use of internet on browsing secured websites and social media. Limited awareness and usage of Virtual Private Networks (VPNs) were evident among participants. And after introducing and explaining our scenario to the participants they seemed to be likely to fall victim to such an attack.

Scenario 2 malicious email attachment

Overall the participant showed a much higher level of awareness of risks and potential dangers when dealing with malicious email attacks in our second scenario than in our 1st scenario, that can be related to either past negative encounters which forced them to learn more about potential email attacks, or that public awareness to email attacks gotten higher in the recent years, but again we cant formulate a conclusion here due to the limited number of participants, the participant showed a good level of caution when opening any link or attachment through their emails and that they usually check and verify the senders details before opening them, finally the participant felt confident in not falling victim to our scenario.

Victim Protection

In this section we will talk about some of the security measures that an individual can take to prevent him/herself from falling victims to each of our proposed scenarios

Protection measures against twin attacks

Here are some of the security measures that can be taken when using public Wi-fi: [5]

1-we should limit access to sensitive information when using public Wi-fi, especially online banking, or online shopping and we try to avoid logging in or using any sensitive login credentials when on public Wi-fi

2-we should steer clear of unsecured Wi-Fi networks, when we search for a Wi-fi network especially when it is an open network, we can see under the name of the network marked as unsecure or secure so we should always avoid accessing networks marked as unsecure.

3- we should use VPNs when using public Wi-fi for maximum security and privacy as VPNs add a level of protection where it encrypts our internet activity before a hacker can see it.

4- when browsing the internet on a public Wi-Fi we should make sure to only use websites that have a URL beginning with 'https' as this refers to encrypted and secured websites.

5- we should disable auto connection as some devices have this option enabled, disabling it will prevent your device from automatically accessing networks with the same name of a network accessed before and fell into a Wi-Fi trap.

6- we should disable file sharing options on our computer before accessing public networks, to keep our files and folders away from other users of the same network.

7- Security managers in the public sector level should initiate educational campaigns targeting the general public, highlighting the risks associated with public Wi-Fi and focusing on creating awareness about the potential dangers of unsecured networks and the importance of cautious behavior.

Protection measures against malicious emails, attachments

Here are some of the security measures that can be taken when using email attachments or links: [6]

1-we should never open a link or an attachment from an untrusted source.

2-we should always check the sender's details when receiving an email with an attachment or a link.

3-we should always use anti-virus on our systems and keep our operating systems updated.

4-we should always be vigilant, aware, and educated of any new tactics that hackers can use through sending malicious emails, and always double check the emails even if they look that they are coming from a trusted source.

Conclusion

In conclusion, as we mentioned earlier the limited number of participants doesn't allow us to conclude solid facts but the exploration of the two scenarios has shed some light on the potential threats of social engineering , both scenarios revealed the importance of user awareness and cautious behavior in mitigating cybersecurity risks. Finally, implementing safe and secure practices that we mentioned above can significantly contribute to overall cybersecurity resilience.

References

1-Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. In 2014 Information Security for South Africa (pp. 1-9). Johannesburg, South Africa. https://doi.org/10.1109/ISSA.2014.6950510

2-Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an ontological model defining the social engineering domain. In 11th Human Choice and Computers International Conference (pp. 266-279). Turku, Finland. https://inria.hal.science/hal-01383064/document

3-Patel, K. C., & Patel, A. (2022). Rogue Access Point: The WLAN Threat. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 943-950). Greater Noida, India. https://doi.org/10.1109/ICCCIS56430.2022.10037591.

4- Email Attachment Threats to Secure Systems From. (2020, May 19). N-Able. https://www.n-able.com/blog/email-attachment-threats-to-secure-your-systems-from

5- What is an evil twin attack? + how to avoid them - Norton. (n.d.). Us.norton.com. https://us.norton.com/blog/emerging-threats/evil-twin-attack

6- Marketing AR, Marketing CWM at P works as a D, writer CWM at PS is a passionate, blogger, Cybersecurity MS in, Technology I. What are Malicious Email Attachments? [Internet]. powerdmarc.com. 2022. Available from: https://powerdmarc.com/malicious-email-attachments/