جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering & Technology

COMP432

COMPUTER SECURITY

Final Report

Instructor: Dr. Mohammad Alkhanafseh

Group members:

- Rasheed S. Alqobbaj – 1202474
- Hassan A. Melhim - 1203289
- Mohammed I. Shabaneh – 1201297

Date: 20/6/2024

Abstract

This report delves into the critical realm of cybersecurity, focusing on the significant threat posed by social engineering attacks. With the increasing interconnectedness of the digital world, protecting data from unauthorized access and manipulation has become paramount for individuals, organizations, and governments. The report examines the fundamental aspects of social engineering, highlighting the methods attackers use to manipulate human psychology and bypass security measures. It studies the case of Evaldas Rimasauskas's $100 million scam against Facebook and Google, illustrating the vulnerabilities and impacts of social engineering. Furthermore, the report discusses the technologies involved, such as OSINT and spear phishing, and presents a comprehensive review of related research papers. The motivation behind the study is to understand the extent to which social engineering threatens cybersecurity and to explore effective countermeasures at technical, managerial, and individual levels. The findings underscore the need for continuous vigilance and enhanced training to mitigate the risks associated with social engineering.

Table of Contents

Introduction

Cyber security is the safeguard of the use of computers, network, programs, and software information from damage, access, attacks, and by other unauthorized personnel or organization. With the internet interconnectedness of the world continues to grow Data security is vital for individuals, organizations, and governments. As a business function Cybersecurity seeks to provide the lenses of confidentiality, integrity and availability on information.

Social engineering is the process whereby one influences a person or a group of people to bypass security features on computers, networks, programs, and information. As societies become progressively connected through the Internet, both at personal and governmental levels, comprehending and countering social engineering threats is crucial. Unlike other cyber threats, social engineering chiefly attacks the psychology of a person, rather than the technological aspect, which makes it a major concern in cybersecurity. Being an emerging component of cybersecurity, social engineering awareness aims to prevent the malicious manipulation of individuals to lose, alter or disclose information in an unauthorized manner.

Key aspects of social engineering:

- Scouting for information, targets, and vulnerabilities.
- Social skills to manipulate, lie, detect social cues.
- Technical skills to use Hacking technique.

Background

Key aspects of social engineering

Scouting for Information, Targets, and Vulnerabilities

This should encompass collection of information on target victims and assessment of their vulnerabilities or rather their security systems. Social engineers, therefore, engage in reconnaissance whereby they gather information like the social identity of a targeted individual, the structure of the targeted organization, and their policies on matters of security. It is possible that the actors would engage in gathering information on the targets by relying on social media and other public records as well as other materials to understand how to leverage their targets most efficiently.

Social Skills for Manipulation, Lying, and Detecting Social Cues

Because social engineers depend on the information given by the people and their ability to put up an outstanding performance. This specifically entails civil intelligence to alter between telling and guessing, a crafty attribute to lie and also read indications. Through it, they manipulate their targets, deceive them, and often impersonate someone their target would know and trust such as a co-worker or someone in the position of authority or even a customer service representative. In this way, they convince people to disclose something personal or contribute to actions that may be dangerous for which he or she will be held responsible.

Technical Skills to Use Hacking Techniques

As a social engineering technique, it majorly revolves around exploiting human psychology but may require technical abilities to perform the attack. This includes the level of skills acquired in hacking methods like sending concurring emails, preparing hazardous software, or mimicking fakes websites. These technical skills are employed by social engineers to supplement the process whereby these criminals engage in deception, thereby making their attacks believable and potent. For example, they might send a message appearing like it has come from a trustworthy internet source with a link to a site embedded in it comprises of malware.

Technologies Involved in Social Engineering

OSINT (Open-Source Intelligence)

OSINT refers to the process of gathering information from publicly available sources to use in an intelligence context. For social engineering, attackers use OSINT to gather details about their targets that can be used to craft convincing spear phishing emails and other types of social engineering attacks.

Key Concepts:

- **Data Sources:** Social media profiles, public records, news articles, forums, and other online resources.
- **Information Gathering:** Collecting information about targets to understand their habits, connections, and vulnerabilities.
- **Exploitation:** Using gathered information to execute targeted attacks.

Spear Phishing

Spear phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific individual, often for malicious reasons, by pretending to be a trustworthy side. Unlike generic phishing attacks, spear phishing emails are personalized and appear to come from a known and trusted source, making them much harder to detect.

Key Concepts:

- **Personalization:** Attackers use information gathered from social media and other sources to personalize their messages.
- **Deceptive Tactics:** Emails often appear to come from legitimate sources, such as colleagues, friends, or trusted companies.
- **Payloads:** Attachments or links in these emails often contain malware or lead to phishing websites designed to steal login credentials.

Research Papers and Opinions

Name	Summary	Opinion
Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks	This study investigates how personality traits, attitudes, and perceived self-efficacy affect vulnerability to spear-phishing attacks. A field experiment conducted in organizational settings revealed that certain personality traits, particularly Conscientiousness, significantly correlate with susceptibility to phishing. Women were found to be more likely to respond to spear-phishing messages than men. Additionally, there was a negative correlation between participants' subjective estimates of their vulnerability and their actual likelihood of being phished. The study suggests that vulnerability to phishing is influenced by personality traits rather than a lack of awareness.	This research provides valuable insights into the psychological factors contributing to phishing vulnerability. I learned that traits such as hardworking play a significant role, which was surprising since I initially thought awareness and training were the main factors. The gender-based differences in response rates were also intriguing. The study highlights the need for targeted defense strategies that consider personality traits, offering a more personalized approach to cybersecurity training and awareness.
Cyber Intelligence & OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media	This paper reviews the use of Open-Source Intelligence (OSINT) in gathering data from publicly available sources, including social media, to profile individuals and organizations for intelligence purposes. The systematic review analyzed 18 research papers and found that social media enhances social cohesion and business opportunities but also presents significant risks. The paper highlights threats such as identity crime, social engineering, and vulnerabilities in HTTP headers and cookies. It emphasizes the need for further research to develop effective mitigation strategies and ensure situational awareness in the use of social media for intelligence gathering.	The systematic review provided a comprehensive understanding of OSINT and its dual role in enhancing and threatening cybersecurity. I learned about the extensive use of social media for intelligence purposes and the associated risks, such as identity theft and social engineering. This research underscores the importance of continuous monitoring and advanced mitigation techniques to counteract the evolving threats in OSINT.
Impact of Social Engineering Attacks: A Literature Review	This literature review explores the significant impacts of social engineering attacks from 2011 to 2020. The findings reveal that social engineering primarily affects companies, financial institutions, and even vehicles, causing economic losses and reputational damage. The review identifies human behavior, such as innocence, unconsciousness, and lack of training, as major causes of vulnerability. The primary victims include newly hired employees, individuals with limited knowledge, celebrities, politicians, and middle to senior managers. Phishing and ransomware are highlighted as the most significant threats.	This literature review provides a broad perspective on the various impacts of social engineering attacks over nearly a decade. I found it particularly insightful that human factors like innocence and lack of training are major contributors to vulnerability. The identification of specific victim profiles, such as new employees and high-profile individuals, was informative. The emphasis on phishing and ransomware as major threats highlights the need for comprehensive training and security measures to protect against these persistent attacks. This review reinforces the critical importance of addressing human factors in cybersecurity strategies.

Case Study: Evaldas Rimasauskas Scamming $100 Million from Facebook and Google

Overview

Evaldas Rimasauskas orchestrated a sophisticated social engineering scam, successfully defrauding Facebook and Google out of $100 million. He impersonated a legitimate hardware vendor and tricked employees into wiring funds to his bank accounts.

Analysis

Rimasauskas executed this elaborate scam by registering a company in Latvia with the same name as Quanta Computer, a legitimate hardware manufacturer in Taiwan frequently used by Facebook and Google. He then created fake email accounts, complete with domain names closely resembling those of Quanta. Using these, he sent phishing emails to employees at Facebook and Google, presenting himself as a representative of Quanta. The emails contained forged invoices, contracts, and other official documents, which appeared legitimate and prompted the employees to wire large sums of money to bank accounts controlled by Rimasauskas.

The scam exploited several vulnerabilities:

- **Lack of Verification Protocols:** Employees failed to verify the authenticity of the emails and the associated requests through independent channels.
- **Over-Reliance on Email Communication:** The companies' reliance on email for processing financial transactions without additional layers of verification or security checks made it easier for the scam to succeed.

Impact

The scam resulted in a significant financial loss and reputational damage to both Facebook and Google. The $100 million loss highlighted the vulnerabilities in their financial transaction processes and the ease with which social engineering tactics could exploit these weaknesses.

In response to the incident, both companies reviewed and strengthened their internal verification protocols and financial transaction processes. They implemented multi-factor authentication for financial transactions and increased employee training on recognizing and responding to phishing attempts. Additionally, they enhanced their cybersecurity measures, incorporating advanced email filtering technologies and verification steps for vendor communications, to prevent similar incidents in the future. This case underscored the importance of robust security protocols and the need for continuous vigilance against social engineering threats.

Motivation and Research Question

Motivation

The motivation for this research stems from the increasing sophistication and frequency of social engineering attacks, which pose significant threats to individuals and organizations. These attacks exploit the fact that humans are often the weakest link in the security chain, as it is often easier for attackers to manipulate individuals than to breach well-defended systems. Additionally, the intriguing role of human psychology and behavior in these attacks highlights the need for understanding and mitigating these vulnerabilities. The interest in social engineering also arises from its significant implications in criminal investigations, where understanding these tactics can aid in solving and preventing crimes.

Research Question

To what degree does social engineering threaten cybersecurity?

Social engineering threatens cybersecurity to a large degree. As seen in our case study and research papers it causes a lot of vulnerabilities in security chains and its implications can cause huge financial damages to various businesses even tech companies, and political strategic information.

Threats and Risks

To explore the severity of damage that social engineering techniques can cause, we will analyze the aforementioned case study, the Evaldas Rimasauskas scam. Evaldas's scam relied on spear-phishing employees to wire funds into his bank account. So, what is spear-phishing? What areas does it attack? Who often uses this form of attack? And how can a company detect it?

Phishing is a type of cyberattack used to extract information by impersonating legitimate companies, institutions, or vendors. Spear-phishing is a targeted form of phishing, considering the victim's background, identity, and career to tailor a phishing attack unique to each target.

Social engineering, and by extension phishing and spear-phishing, extract information that malicious users can exploit to attack in various ways:

- **Financial Loss**: Deceiving users into transferring funds. For example, an email seemingly from the company's CEO is sent to the finance department, instructing them to transfer funds to a new vendor account.
- **Data Breach**: Extracting confidential information that might be used for blackmail or identity fraud. For instance, an HR manager receives a job application with an attachment named "Resume." The attachment contains malware that, once opened, extracts employee information such as social security numbers, salary details, etc.
- **Reputation Damage**: Information leaks that severely damage the trust between a company and its investors. For example, a PR officer receives an email from a reputable journalist inquiring about exclusive information to prepare for an article. The imposter journalist then leaks the information ahead of time.
- **Operational Disruption**: Certain operations and processes can be halted due to a compromised system. For instance, an IT administrator at a hospital receives an email titled "Mandatory update installation," which installs ransomware that encrypts patient records.

Social engineering targets human users and originates from them. Attackers are called Threat Actors; they can be categorized into three groups depending on their motivation:

- **Cybercriminals**: Motivated by financial gain.
- **Nation-State Actors**: May seek to disrupt or gain strategic advantage.
- **Insider Threats**: Employees who may be compromised or act maliciously.

Similarly to how cyber defenses have security policies to defend against cyber-attacks, there are also security policies to defend against social engineering attacks. Because attacks done through social engineering are dependent on human error, security policies aim to teach users how to detect attacks.

Focusing on phishing attacks as per our case study, a few detection methods can decrease the likelihood that employees fall victim to such attacks:

- **Email Filtering**: Filtering suspicious emails, such as those with incoherent email addresses.
- **Raising Awareness**: Informing users about what their employees are allowed and not allowed to ask for.
- **Employee Education**: Training employees to detect phishing attempts.

Countermeasures

After defining the effects, origins, and methods of social engineering attacks, we next analyze potential solutions to mitigate these attacks. The solutions are divided into three types based on the level at which they operate: Technical level, Managerial level, and Individual level.

Technical Level

The Technical level refers to technical measures implemented to ensure certain actions cannot be performed due to coercion or to act as obstacles to the Threat Actors, deterring them from succeeding. Examples of countermeasures at the technical level include:

- **Multi-Factor Authentication (MFA)**: Adds an additional layer of security.
- **Advanced Email Filtering and Security**: Using AI to detect and block phishing emails.
- **Endpoint Protection**: Securing devices with antivirus and anti-malware software.

Managerial Level

The Managerial level refers to company policies created by the management divisions in an organization. These policies are meant to equip staff with tools and knowledge to detect and avoid these attacks. Examples include:

- **Regular Training Programs**: Educating employees on identifying and responding to phishing attacks.
- **Incident Response Plan**: Having a clear, actionable plan in place for when an attack is detected.
- **Access Controls**: Implementing the principle of least privilege to limit access to sensitive information.

Individual Level

The Individual level refers to best practices an employee or user might uphold to decrease the likelihood of an attack targeting them. Examples include:

- **Regular Software Updates**:
  - **Example**: Ensure that operating systems, applications, and antivirus software are updated promptly to protect against known vulnerabilities.
- **Secure Communication Channels**:
  - **Example**: Use encrypted email services and secure messaging apps for sensitive communications to prevent interception by malicious actors.
- **Verify Requests for Sensitive Information**:
  - **Example**: Always verify requests for sensitive information or financial transactions by contacting the requester through a different communication channel before acting.
- **Strong Password Practices**:
  - **Example**: Use complex, unique passwords for different accounts and change them regularly. Consider using a password manager to keep track of them securely.
- **Beware of Suspicious Links and Attachments**:
  - **Example**: Hover over links to check their actual destination before clicking and avoid opening attachments from unknown or unexpected sources.
- **Monitor Accounts Regularly**:
  - **Example**: Regularly check bank statements, credit reports, and online accounts for any unauthorized activity and report discrepancies immediately.
- **Limit Personal Information Sharing**:
  - **Example**: Be cautious about sharing personal information on social media and other public forums, as this information can be used to craft targeted phishing attacks.
- **Regular Backups**:
  - **Example**: Regularly backup important data to a secure, offline location to ensure data recovery in case of a ransomware attack.
- **Stay Informed**:
  - **Example**: Keep up to date with the latest security news and trends to be aware of new phishing techniques and threats.

Future Trends and Challenges

The world of technology is ever-growing, and with every new development comes new vulnerabilities and newer tactics. Currently, the trend is in all things AI, which poses a large challenge when defending against social engineering attacks. Moreover, more effective targeting by Threat Actors serves as another example of challenges regarding the prevention of attacks through social engineering.

Using Artificial Intelligence, Threat Actors are able to construct more convincing phishing emails in shorter time and larger numbers, thus ensuring that at least one attack might be overlooked and breach the system. Also, the use of Deepfake technology to synthesize media raises the intricacy of the impersonations.

The increase in remote jobs has sparked new vulnerabilities and created new opportunities in which Threat Actors can exploit. Remote workers often neglect the security of their home networks and use personal devices that do not possess the same security protections as company devices. Moreover, the lack of personal engagement of staff in an online environment leads remote workers to be more susceptible to being fooled by impersonators.

Conclusion

In conclusion, social engineering remains a formidable challenge in the field of cybersecurity, exploiting the inherent vulnerabilities of human psychology rather than technological defenses. The sophisticated attack orchestrated by Evaldas Rimasauskas against Facebook and Google underscores the significant financial and reputational damage that can result from such tactics. Through detailed analysis and examination of various research studies, it is evident that personality traits, gender differences, and a lack of awareness contribute to the susceptibility of individuals to these attacks. The report highlights the importance of comprehensive countermeasures, including regular software updates, advanced email filtering, and robust employee training programs. As technology evolves, so do the methods employed by threat actors, making it imperative for organizations to stay informed and proactive in their defense strategies. By addressing the human element and implementing multi-faceted security protocols, it is possible to significantly reduce the risk and impact of social engineering attacks, safeguarding critical information and maintaining trust in digital interactions.

References

- Cyber Intelligence & OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media Yeboah-Ofori, Abel. (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. International Journal of Cyber-Security and Digital Forensics. 7. 87-98. 10.17781/P002378.
- Evaldas Rimasauskas Scamming $100 Million from Facebook and Google Jr., Tom Huddleston. “How This Scammer Used Phishing Emails to Steal over $100 Million from Google and Facebook.” *CNBC*, CNBC, 27 Mar. 2019.
- Impact of Social Engineering Attacks: A Literature Review Fuertes, Walter & Arévalo, Diana & Castro, Joyce & Ron, Mario & Estrada, Carlos & Andrade, Roberto & Peña, Felix & Benavides, Eduardo. (2022). Impact of Social Engineering Attacks: A Literature Review. 10.1007/978-981-16-4884-7_3.
- Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks Halevi, Tzipora & Memon, Nasir & Nov, Oded. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. SSRN Electronic Journal. 10.2139/ssrn.2544742.