ISSN: 2454-9940

IJASEM

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijsem.org
Vol 11, Issuse. 2 June 2020

UNMASKING SOCIAL ENGINEERING ATTACKS ON DATA

Mr. C. Santhosh Kumar Reddy, MCA, *1
Mrs. S. Madhavi. MSC in Computer Science , *2
Mr. K. Sreedhar, MCA, *3

ABSTRACT:

The Social engineering attacks is the trick unsuspecting users into clicking on malicious links or providing their confidential information. This information is then used for various malicious purposes, including identity theft, financial fraud, or unauthorized access to sensitive accounts.

This abstract will provide how we unmasking the social engineering attacks by creating an application using salesforce. Where we develop an application provides a platform called Salesforce AppExchange, to detect the Social engineering attacks.

INTRODUCTION:

With the significant growth of internet usage, people increasingly share their personal information online. As a result, an enormous amount of personal information and financial transactions become vulnerable to cybercriminals.

The increasing reliance on technology and interconnected systems has provided opportunities for cyber-attacks to evolve beyond traditional methods such as hacking and malware. Social engineering attacks exploit human psychology and trust in order to deceive individuals into divulging sensitive information, performing unintended actions, or compromising security measures.

The motivation behind social engineering attacks can vary. Some attackers may seek financial gain, aiming to steal banking information, credit card details, or personal identities for financial fraud or identity theft. Others may target intellectual property or trade secrets to gain a

1. **Faculty, Department of Computer Science Siva Sivani Degree College, Kompally, Sec'bad-100**
2. **HOD in Department of Computer Science Siva Sivani Degree College, Kompally, Sec'bad-100**
3. **Faculty, Department of Computer Science Siva Sivani Degree College, Kompally, Sec'bad-100**

competitive advantage or sell sensitive information on the black market. Additionally, nation-states may employ social engineering attacks to gather intelligence or disrupt critical infrastructures of other nations.

There are various techniques employed in social engineering attacks. Phishing is one of the most prevalent methods, where attackers send fraudulent emails or messages impersonating trusted entities, and on clicking on malicious links or providing confidential data.

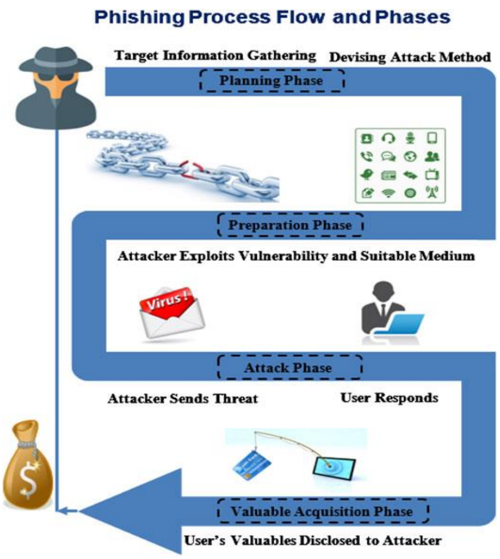
Phishing Process Flow and Phases
Target Information Gathering
Devising Attack Method
Planning Phase
Preparation Phase
Attacker Exploits Vulnerability and Suitable Medium
Virus!
Attack Phase
Attacker Sends Threat
User Responds
Valuable Acquisition Phase
User's Valuables Disclosed to Attacker

FIGURE 1: Phishing attack types and techniques drawing upon existing phishing attacks.

One of the social engineering attacks phishing. The following figure shows how phishing process flow and phases

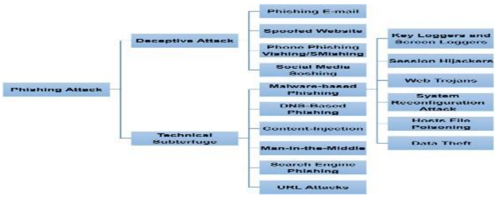

FIGURE 2: Phishing attack types and techniques drawing upon existing phishing attacks.

ALGORITHMS AND TECHNIQUES

There are various algorithms and techniques used in AI to detect social engineering attacks. Here are a few commonly employed methods:
1. **Natural Language Processing (NLP):** NLP algorithms analyse text and language patterns to identify suspicious or manipulative content. They can detect phishing emails, scam messages, or social media posts that attempt to deceive or manipulate users.
2. **Machine Learning (ML):** ML algorithms can be trained on large datasets of known social engineering attacks to learn patterns and characteristics of such attacks. These algorithms can then be used to classify and detect new instances of social engineering attempts.
3. **Anomaly Detection:** Anomaly detection algorithms identify deviations from normal behaviour or patterns. They can be applied to user behaviour, network traffic, or communication patterns to detect unusual or suspicious activities that may indicate a

social engineering attack.

4. **User Profiling:** AI algorithms can create user profiles based on behaviour, preferences, and historical data. By comparing current user behaviour to their established profile, any deviations or inconsistencies can be flagged as potential social engineering attempts.

5. **Social Network Analysis:** Social network analysis algorithms examine relationships and interactions between individuals or entities to identify suspicious patterns or connections. They can help detect social engineering attacks that involve impersonation or manipulation within a network.

METHODOLOGY

1.EXISTING METHODOLOGY

Social engineering attacks entail the use of trickery and manipulation to get sensitive data or unapproved access to systems. This is a typical approach to social engineering attacks:

There are several existing methodologies for unmasking social engineering attacks on data, here are a few commonly used approaches:

1. Employee Training and Awareness: Educating employees about social engineering tactics, such as phishing emails or phone scams, can help them recognize and report suspicious activities. Regular training sessions and awareness campaigns can enhance their ability to identify and mitigate potential threats.

2. Incident Response and Monitoring: Implementing robust incident response procedures and monitoring systems can help detect and respond to social engineering attacks. This includes monitoring network traffic, analysing logs, and employing intrusion detection systems to identify any unauthorized access attempts or suspicious behaviour.

3. Multi-factor Authentication (MFA): Enforcing MFA adds an extra layer of security by requiring users to provide additional verification factors, such as a fingerprint or a one-time password, in addition to their regular credentials. This can help prevent unauthorized access even if an attacker manages to obtain login credentials through social engineering.

4. Security Awareness Programs: Organizations can conduct security awareness programs to educate employees about the risks associated with social engineering attacks. These programs can include simulated phishing campaigns, where employees are sent fake phishing emails to test their response and provide targeted training based on the results.

5. Incident Response Planning: Developing a comprehensive incident response plan that includes specific steps to address social engineering attacks can help organizations respond effectively and minimize the impact of such incidents. This plan should outline roles and responsibilities, communication protocols, and steps for containment, eradication, and recovery. It is important to note that no method is fool proof, and a combination of these approaches, along with regular updates and improvements, is recommended to effectively combat social engineering attacks on data

Spam mails, also known as unsolicited bulk emails, are a common nuisance and can pose security risks. Here are some ways to deal with spam mails:

1. Enable Spam Filters: Most email providers offer built-in spam filters that automatically detect and filter out spam emails. Make sure to enable and regularly update these filters to reduce the number of spam mails reaching your inbox.

2. Be cautious with your email address: Avoid sharing your email address publicly or on untrusted websites. Spammers often scrape the internet for email addresses, so limiting its exposure can help reduce the amount of spam you receive.

3. Don't reply or click on dubious emails: Steer clear of replying to or clicking on dubious emails' links or attachments. By doing this, you may be encouraging more spammers by confirming to them that your email address is active. Such emails should be deleted right away.

4. Report spam: Most email providers have options to report spam emails. By reporting spam, you help improve the effectiveness of spam filters and contribute to reducing spam for others.

Remember, while these measures can help reduce spam, it is impossible to completely eliminate it. Staying vigilant and employing good email practices can go a long way in minimizing the impact of spam mails.

PROPOSED METHODOLOGY

A proposed system for unmasking social engineering attacks on data could involve the following components:
1. Email and Web Filtering: Implementing robust email and web filtering mechanisms can help block malicious emails, phishing websites, and other social engineering vectors. These filters can analyse email content, URLs, and attachments to identify and block suspicious or malicious content

2.Artificial Intelligence and Machine Learning: Utilizing AI and machine learning algorithms can enhance the system's ability to detect and respond to social engineering attacks. By providing web links using These algorithms can learn from historical data and identify patterns or anomalies that may indicate a potential attack which will detect the links .They can also continuously adapt and improve their detection capabilities based on new information.

There are various machine learning algorithms that can be used in unmasking social engineering attacks in data. Here are a few commonly employed algorithms:

1. Anomaly Detection: Anomaly detection algorithms, such as Isolation Forest, One-Class SVM, or Autoencoders, can be used to identify unusual patterns or behaviors in data. These algorithms can help detect anomalies that may indicate social engineering attacks, such as unauthorized access attempts or abnormal user behavior.
2. Classification Algorithms: Classification algorithms, such as Decision Trees, Random Forests, or Support Vector Machines (SVM), can be trained on labeled datasets to classify instances as either legitimate or malicious. By analyzing various features and patterns in the data, these algorithms can help identify social engineering attacks based on known patterns.

3. Natural Language Processing (NLP) Techniques: NLP techniques, such as sentiment analysis, text classification, or named entity recognition, can be applied to analyze textual data, such as emails or chat logs, for signs of social engineering attacks. These techniques can help identify suspicious or manipulative language used by attackers.

4. Deep Learning Models: Deep learning models, such as Recurrent Neural Networks (RNNs) or Convolutional Neural Networks (CNNs), can be utilized to analyze and detect patterns in large volumes of data. These models can be trained on labeled datasets to identify social engineering attacks based on learned patterns and features.

A combination of multiple algorithms and techniques may be employed to enhance the accuracy and effectiveness of the detection system. Regular updates and improvements to the algorithms are also necessary to adapt to evolving attack techniques.

Salesforce tools for cyber attacks

We create an application using Salesforce to detect Social engineering attacks.

Salesforce provides a platform called Salesforce AppExchange, where you can find and install various applications developed by Salesforce and their partners.

To develop an application specifically for detecting phishing, you would need to use Salesforce's development platform, known as Salesforce Lightning Platform (previously known as Force.com). Within this platform, you can use tools like Salesforce Apex (a Java-like programming language), Visualforce (a mark-up language for building user interfaces), and Salesforce Lightning Components (a framework for building modern web applications).

Here are the general steps to create a social engineering detection application using Salesforce:

1. Define requirements: Determine the specific features and capabilities the application should have for detecting phishing attempts.

2. Design the application: Create a high-level design of the user interface and functionalities based on the requirements.

3. Develop the application: Use Salesforce Apex to write code for implementing the detection algorithms and rules. Use Visualforce to create the user interface for the application.

4. Test the application: Perform various tests to ensure the application is working as expected.

5. Deploy the application: Package the application and deploy it to a Salesforce org.

6. Publish the application: If you want to make the application available to others, you can publish it on the Salesforce AppExchange. This will allow other Salesforce users to install and use your application.

Conclusion:

Social engineering attacks using web links continue to pose a serious threat to data security. Recognizing the tactics employed by attackers and implementing proactive measures is crucial in mitigating risks. By combining user education, advanced technological solutions, and a vigilant approach, organizations can strengthen their defences against social engineering attacks and safeguard sensitive information from unauthorized access. The effectiveness of countermeasures may evolve with emerging threats, emphasizing the need for continuous monitoring, adaptation, and collaboration between technology, training, and organizational policies to stay ahead of cyber adversaries.

References

[1] A Cybersecurity Agenda for the 45th President. (2017, January 5). Retrieved from https://www.csis.org/news/cybersecurity-agenda-45th-president

[2] Zhang, T. (2017). Understanding Machine Learning: From Black Box to White Box. Springer

[3] https://developer.salesforce.com

[4] ussell, S. J., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Pearson.

[5] halev-Shwartz, S., & Ben-David, S. (2014). Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press.

[6] Trailhead | The fun way to learn (salesforce.com)

[7] Witten, I. H., Frank, E., & Hall, M. A. (2016). Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann.