Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 9 September 2023

Review Article

Social Engineering as A Tool for Cyber-Attacks

Ruchika Lalit[1], Priyanka Bhutani[2], Neha Verma[3]* and Sarthak Marwah[1]

[1]*The NorthCap University, Gurugram, India*

[2]*University School of Information, Communication and Technology (USIC and T), Guru Gobind Singh Indraprastha University (GGSIPU), India*

[3]*VIPS (Member of CSD), Guru Gobind Singh Indraprastha University (GGSIPU), India*

***Corresponding Author:** Neha Verma, VIPS (Member of CSD), Guru Gobind Singh Indraprastha University (GGSIPU), India.

Received: August 14, 2023

Published: August 22, 2023

Abstract

As technology advances and cybersecurity measures become more sophisticated, cybercriminals are increasingly turning to social engineering tactics to gain access to sensitive information or systems. Social engineering refers to the tactic of taking advantage of human weaknesses to accomplish harmful goals, which may involve deceiving people into revealing sensitive information or breaching security measures.

This approach has proven to be highly effective and is responsible for a significant portion of cyber-attacks. Unfortunately, many victims are unaware that they are being manipulated and may inadvertently sabotage the system themselves. Social engineering refers to a variety of malicious tactics that rely on human interactions to deceive and manipulate individuals into divulging confidential information or committing security breaches. Such attacks usually occur in multiple stages, starting with the perpetrator conducting research on the target to identify vulnerabilities and weaknesses in their security protocols. The attacker then gains the victim's trust by using various psychological tactics and provides incentives to encourage actions that compromise security, such as revealing sensitive data or granting unauthorized access to critical resources. It offers a formal and clear knowledge schema to comprehend, examine, reuse, and exchange social engineering domain knowledge. Cyber attackers use social engineering tactics to manipulate individuals to divulge sensitive information or to perform actions that may compromise a system's security. Throughout this paper, we explore various forms, strategies, and consequences of social engineering, which in turn supports Sustainable Development Goals (SDG-9). The paper also examines the effectiveness of different countermeasures and strategies for preventing social engineering attacks. By analyzing the latest research and real-world examples, this paper aims to increase awareness and understanding of social engineering, and help individuals and organizations better protect themselves from this growing threat.

Keywords: Social Engineering; Cyber- Attack; Cyber Security; Phishing; Baiting

Introduction

Social engineering is a technique employed in computer and cyber security to exploit human weaknesses, such as susceptibility to persuasion, deception, manipulation, and coercion, to gain access to confidential information, breach security measures, and hack computer systems and networks [1]. The aim of such attacks is to undermine the confidentiality, integrity, controllability, availability, and auditability of various components of cyberspace, such as infrastructure, resources, data, operations, and users [2]. Essentially, social engineering involves leveraging human weaknesses through social interaction to exploit vulnerabilities and jeopardize the security of cyberspace [3-5]. Although these kinds of attacks are a threat to organizations, they can be challenging to counter since they exploit human weaknesses rather than technological ones [6]. The FBI has observed a significant increase in CEO fraud and email scams, where attackers impersonate executives and request funds transfers through emails sent to select employees. These fraudulent activities have resulted in businesses losing over $2.3 billion. Moreover, recent research studies and surveys have highlighted that social engineers succeed in executing 84% of cyberattacks [7]. These statistics and others demonstrate that social engineering attacks can result in higher costs than natural disasters, emphasizing the importance of detecting and preventing such cyberattacks.

Hence, it is pertinent that the organizations lay emphasis on educating their employees about the risks of social engineering and provide training on how to detect and prevent such attacks. Implementing security measures like network segmentation and two-factor authentication can also help reduce the risk of social engineering attacks.

Forms of social engineering

Cybercriminals frequently utilize social engineering to take advantage of human emotions, trust, and lack of knowledge for gaining access to secure systems or sensitive information [3,4]. These attacks can manifest in various forms, such as phishing emails, pretexting, baiting, and quid pro quo. Phishing emails typically involve the use of fraudulent messages to deceive individuals into clicking on a link or downloading an attachment that can install malware or lead them to a bogus website that captures login credentials. Pretexting involves fabricating a fake scenario that requires personal information, such as impersonating a bank representative to acquire account details. Baiting entails leaving a physical device, like a USB stick which installs malware, in a public area, with the intention that a naïve person picks and plugs the device into their system. Quid pro quo is the type of social engineering attack in which the employee is offered something in exchange for sensitive information, such as providing a gift card in lieu of accessing the organization's network.

Basic mechanism of a social engineering attack

The basic mechanism of a social engineering attack in shown in figure 1 and detailed below

- **Research:** The attacker first researches the target and gathers as much information as possible, such as their job title, role, and personal information. They may use online sources, such as social media or public records, to gather this information.
- **Pretexting:** The attacker then creates a false identity or pretext, such as posing as a customer service representative, IT support, or a trusted colleague. Using this pretext, they gain the trust of the target.
- **Building rapport:** The attacker builds rapport with the target by using social engineering techniques such as flattery or finding common interests. As a result, the target's guard is lowered and trust is created.
- **Creating urgency:** Attackers then threaten to close the target's account or tell them that their computer has been hacked to create a sense of urgency or fear in the victim. This sense of urgency makes the target more likely to act quickly without thinking things through.
- **Requesting action:** The attacker then requests that the target take a specific action, such as providing their login credentials, downloading malware, or transferring money. The request may appear legitimate due to the attacker's established trust and use of pretexting.
- **Successful attack:** Scammers gain access to sensitive information or control the system if the target falls for the scam. These pieces of information are then used by the attacker to do further attacks or make financial gains.

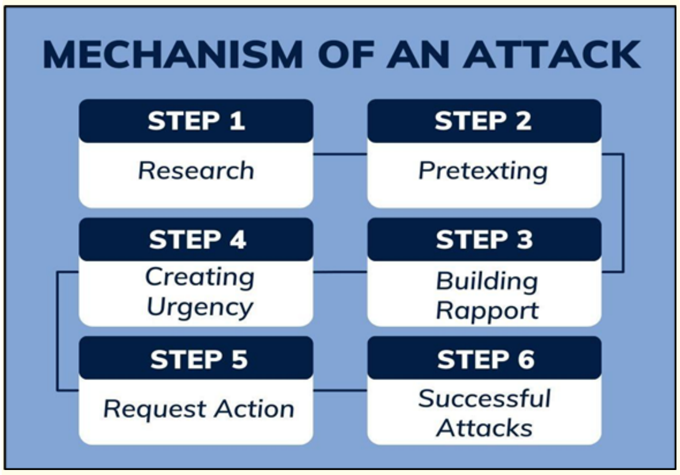


Figure 1: Mechanism of a Social Engineering attack.

Attack vectors

An attack vector is a method through which the attacker can take advantage of flaws in the system, which may also involve human element weaknesses. It can be either a social strategy alone or a socio-technical approach involving both social and technical aspects. The social strategy attack vectors are explained in section 4.1. The socio-technical attack vectors are provided in section 4.2.

Social strategy

Social engineering attacks can manifest through various actions, such as tailgating, posing as another person, listening in on conversations, eavesdropping, shoulder surfing, and dumpster diving, among other methods.

Tailgating

Tailgating refers to the act of following an authorized individual through a secure door into a restricted area without proper clearance. This can be achieved by either requesting the person to hold the door open or by quickly entering before the door closes. With smoking prohibited in many company premises due to safety and health regulations, tailgating has become more effective as it enables attackers to target groups of smokers and utilize social engineering tactics.

Impersonating

"False identity" is a social engineering technique in which a threat actor assumes a fabricated persona to execute malicious actions. This tactic may involve methods such as pretexting, quid pro quo and piggybacking. Piggybacking refers to gaining entry into secure areas by posing as personnel or businesses that require temporary access. Pretexting involves creating a believable scenario to engage the target and bypass security protocols, such as posing as an authority figure or trusted entity to obtain personal information and credentials. This tactic requires extensive research on the target to develop a credible story that doesn't raise suspicion. Quid pro quo is a attack where the attacker masquerades as an IT support technician, offering assistance to a victim facing technical issues in exchange for sensitive information, with the goal of infecting the targeted system.

Eavesdropping

In situations where only authorized personnel are permitted, sensitive information may be casually discussed within a company. Exploiting this security loophole does not require threat actors to be physically present. They can also actively monitor communication channels, such as phone lines and email accounts, to gain access to confidential information.

Shoulder surfing

The practice of shoulder surfing involves directly observing and gathering personal information by peeking over a victim's shoulder, typically with the intention of obtaining authentication data.

Dumpster diving

Rummaging through garbage has long been a tactic employed by attackers to uncover confidential information. It is common for both individuals and organizations to inadequately dispose of physical materials such as paperwork or hardware, which can be exploited to extract sensitive data.

Reverse social engineering

To avoid arousing suspicion, the attacker entices the target to initiate contact while remaining hidden. They create a fake problem for the victim, adopt a persona that appears credible, and ultimately provide a viable solution.

Socio-technical approach

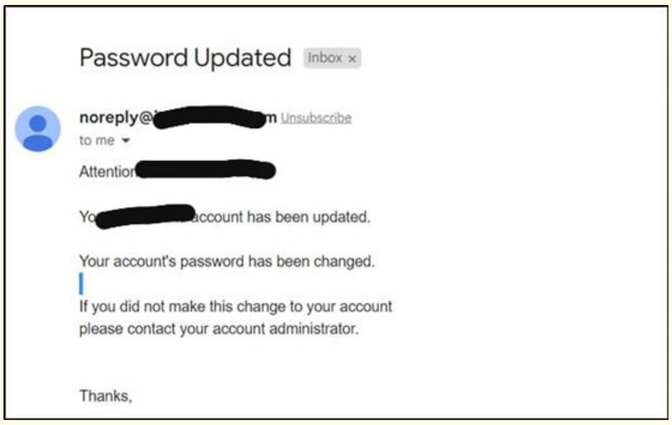
Various situations can give rise to the social-technical approach, including but not limited to baiting, watering hole attacks and phishing.

Phishing

Attacks of phishing use various digital methods, including fraudulent emails and websites that mimic trusted sources, to obtain personally identifiable information from unsuspecting victims. Advanced phishing scams often manipulate the victim's psychological vulnerabilities to create a false sense of urgency, clouding their judgment (figure 2). While phishing attacks aim to target as many individuals as possible, spear-phishing is a more focused approach that requires prior research to craft personalized messages for each target. Cybercriminals may use social media platforms to collect information about potential victims and create convincing communications that appear to be from acquaintances or friends.

Watering hole

The described method of social engineering is particularly advanced as it requires a significant amount of technical skill. The attacker conducts thorough research to identify reputable websites that the target frequently visits. They carefully assess these websites to identify vulnerabilities, and then exploit the most strategically advantageous one to launch the attack, before patiently awaiting the desired outcome.



Password Updated

noreply@[redacted]

to me ▾

Attention[redacted]

Yo[redacted]account has been updated.

Your account's password has been changed.

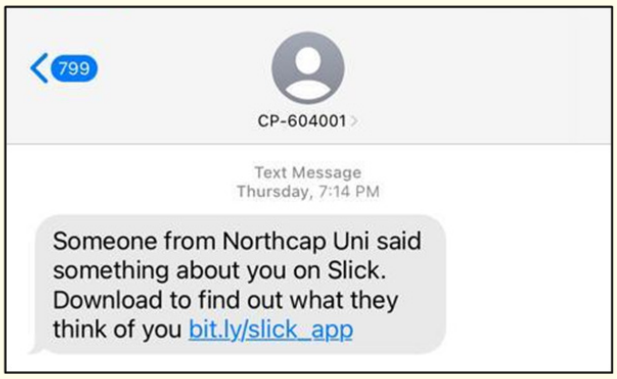
If you did not make this change to your account
please contact your account administrator.

Thanks,

Figure 2: Tricking Phishing Mail.

Baiting

A physical attack vector that can be utilized by attackers involves infecting a storage device with malware and intentionally leaving it for the targeted victim to discover. The victim may inadvertently plug the infected device into their system, which can lead to the execution of the malware (Figure 3).



CP-604001

Text Message
Thursday, 7:14 PM

Someone from Northcap Uni said something about you on Slick. Download to find out what they think of you bit.ly/slick_app

Figure 3: Baiting to click on that Link.

Categories

According to their approach and methodology, social engineering attacks can be classified into two categories: hunting and farming.

Hunting

The primary objective of this approach is to execute a social engineering attack with minimal interaction with the target person. Once the attacker has achieved their desired result and confirmed the security breach, they typically end all communication with the victim. This approach is frequently employed to facilitate cyberattacks, and often relies on a solitary interaction as the mode of operation.

Farming

While not a frequently used technique, social engineering farming can be effective in specific situations. The attacker's goal with this strategy is to establish a relationship with the victim and gather information over an extended period of time. As the interaction progresses, the dynamics may shift, and the target may become aware of the deception, forcing the social engineer to resort to conventional criminal tactics like bribery or blackmail.

Attack cycle

The complexity of social engineering attacks can differ, ranging from simple single interactions to multi-stage operations involving several threat actors gathering information from various sources, all aimed at achieving a specific goal (figure 4). Despite the variation, even attacks relying on a single interaction usually follow four distinct phases: Investigation, Hook, Play, and Exit [10].

Investigation

The probability of success of most attacks depends on this stage, so it is natural that attackers spend most of their time and attention on it. A social engineering attack is carried out by gathering information about the target's digital presence and security systems to identify potentially exploitable vulnerabilities. This may involve conducting reconnaissance on the target's website, email accounts, social media profiles, and any other online presence. During the research phase, the attacker may also try to identify the software and hardware used by the target and any potential security weaknesses associated with them. For example, they may search for vulnerabilities in the target's operating system, network infrastructure, or software applications.

Hook

A threat actor initiates communication with the potential victim during this phase. By creating false narratives and establishing a connection, the attacker earns the trust of the target and takes advantage of the situation to start a discussion.

Play

In Play phase, the attacker performs an attack to strengthen their position. Their actions would be directed towards stealing or disrupting important and confidential information, depending on their goals.

Exit

The Exit phase marks the end of the social engineering lifecycle. At this stage, the Social Engineer endeavors to cover their tracks and erase any evidence of their activities. Armed with the knowledge and information gained from the previous attack cycle, the attacker will employ more advanced techniques to target and deceive their next victim.

A Social-technical example

In this Segment, we will demonstrate the step-by-step procedure of a technological attack using a simple example. To do so, we will utilize the SocialPhish tool that is already included in Kali Linux (Figure 5).

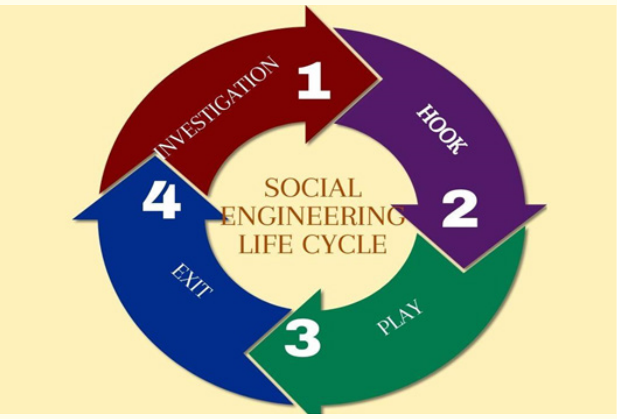
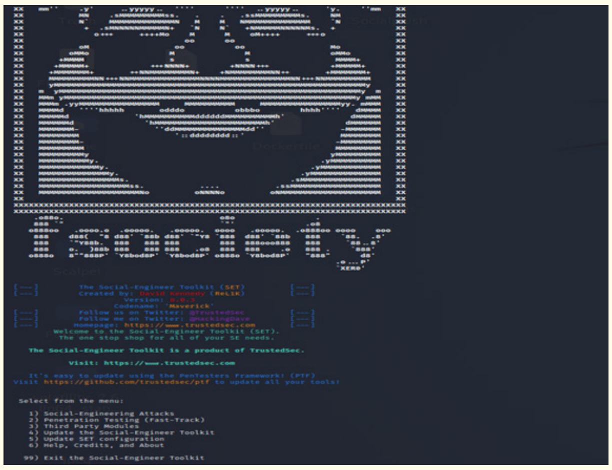


Figure 4: The Life Cycle of a Social Engineering attack.



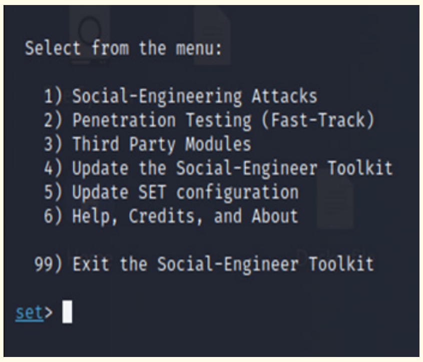
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                    Version: 8.0.3
                  Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit
```

Figure 5: Screen after opening the Social Engineering Toolkit (SET).

Kali Linux [8] is an operating system that is free and open source, which is mainly used for penetration testing. It is based on Debian Linux and comes equipped with a variety of tools to detect and take advantage of system vulnerabilities. Offensive Security is responsible for developing and maintaining this operating system, which has gained popularity among cybersecurity enthusiasts and professionals.

The Social-Engineer Toolkit (SET) is another commonly used tool in the cybersecurity community, with over two million downloads [9] (Figure 6). It is an open-source, menu-driven tool that facilitates penetration testing. SET has become the industry standard for executing advanced technical attacks in social engineering scenarios and can be easily launched on Kali Linux by typing "setoolkit" into the terminal. SET was created by TrustedSec.

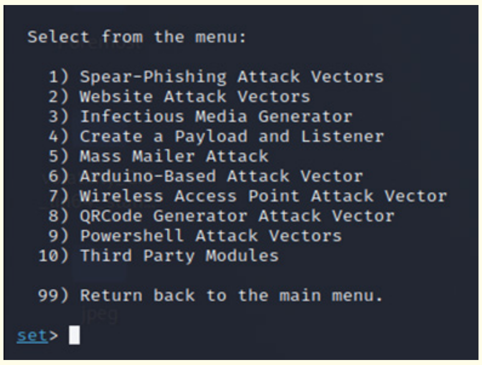
Once launched, SET presents users with a main menu consisting of six options and an exit button. This study focuses on social engineering attacks, and therefore, the attack demonstration centers around the first option in the menu, which is social engineering attacks. Within this option, the "Website Attack Vec-



```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 
```

Figure 6: TOOLKIT MENU.

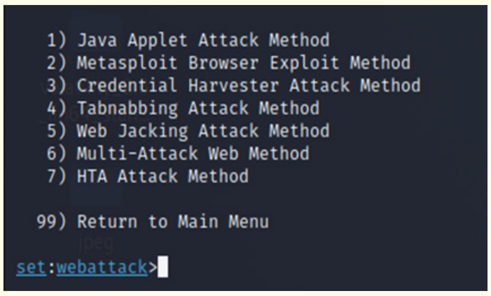
tors” is selected to showcase a simple phishing attempt based on a website (Figure 7).



```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 
```

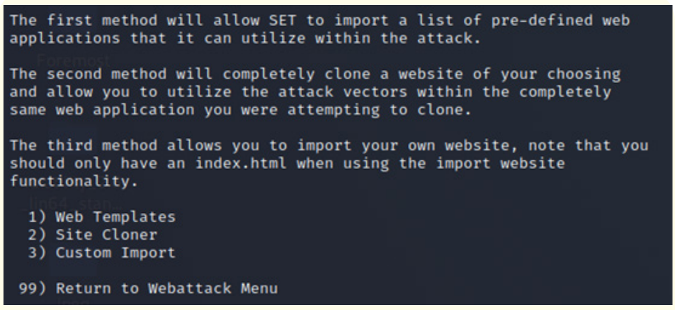
Figure 7: Social engineering attack MENU.

The attacker proceeds with the instructions provided by the Social-Engineer Toolkit to gain access to a victim’s credentials. To achieve this, the attacker selects the “Credential Harvester Attack Technique” from the website attack vectors menu, which is the third option (as depicted in Figure 8). The objective is to obtain the desired credentials. The exploit attempt is represented by the second procedure in this menu, shown in figure 9.



```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>
```

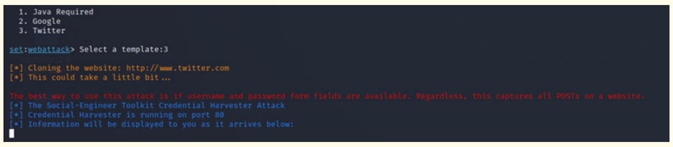
Figure 8: Website Attack Menu.



```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu
```

Figure 9: Credential Harvester Menu.

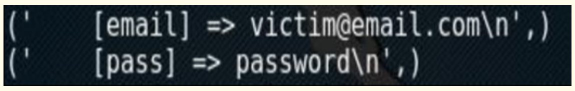
An attack method exists that involves creating a fake version of a website with the aim of stealing login credentials from a specific target. To carry out this type of attack, the perpetrator needs to input the website’s URL66 and the IP55 address of their attack system, such as Kali Linux (192.168.70.128). As an illustration, let’s suppose that the target website is Twitter (as shown in figure 10)



```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Figure 10: Credential Harvester Attack.

In the final step, the perpetrator deceives the victim by sending a fake link that leads to a duplicated web platform (as shown in figure 11). Through skillful social engineering tactics, the attacker is able to manipulate the victim into entering incorrect login credentials. The Kali Linux server receives the victim’s username and password when they click the link.



```
('    [email] => victim@email.com\n',)
('    [pass] => password\n',)
```

Figure 11: Login Credentials.

Precautions

- Hackers can easily access confidential information if people use the same password across several accounts.
- In order to prevent social engineering attacks, it is critical to use strong passwords containing uppercase, lowercase, and special characters.
- Another precaution is to avoid giving your phone or laptop to anyone you don’t trust, as they may try to access your accounts or install malicious software.
- Many websites offer security questions as an added layer of protection, as these questions are difficult to crack. It is also essential to avoid visiting suspicious websites or clicking on unknown links, as these may lead to infected pages.

- Two-factor authentication is a useful tool offered by many social media sites to prevent hacking attempts.
- Always verify the URL of a website before using it, and look for the HTTPS secure certificate to ensure it is safe.
- Installing antivirus software can help protect against malware that attackers may try to install through social engineering. Additionally, it is important to never open emails from unknown senders, as phishing and baiting attacks often come through email. Finally, remember to always log off accounts when finished using them, as hackers may take advantage of stored cookies to gain access to your social media accounts.

Conclusion

The Information Age has progressed to a stage of maturity where the Internet is widely used and has driven rapid evolution in human knowledge and society. Consequently, people have become reliant on the World Wide Web, and the digital realm has become a platform for various criminal activities. Although cybersecurity measures have advanced in complexity, individuals remain highly susceptible to cybercrime. Recent research has shown that a vast majority of cyber-attacks result from human vulnerabilities, with threat actors increasingly exploiting social engineering techniques. Therefore, the innovation of social engineering is likely to remain the most dominant attack vector in the future of cybersecurity, and additional research is necessary to inform best practices and measures for both individuals and organizations as well as satisfies the Sustainable Development Goals (SDG-9), Industry Innovation Infrastructure.

Bibliography

1. Ahmed R and Dharaskar RV. “Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective”. In *6th International Conference on E-Governance, Iceg, Emerging Technologies in E-Government, M-Government* (2008): 312-323.

2. Raheja S and Munjal G. “Classification of Microsoft Office Vulnerabilities: A Step Ahead for Secure Software Development”. In: Bhoi, A., Mallick, P., Liu, CM., Balas, V. (eds) Bio-inspired Neurocomputing. Studies in Computational Intelligence. Springer, Singapore 903 (2021).

3. Wang Z., *et al*. “Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods”. *IEEE Access* 9(2021): 11895-11910.

4. Lohani S. “Social engineering: Hacking into humans”. *International Journal of Advanced Studies of Scientific Research* 4.1 (2019).

5. Wang Z., *et al.* “Social engineering in cybersecurity: a domain ontology and knowledge graph application examples”. *Cybersecur* 4 (2021): 31.

6. Breda F., *et al.* “Social engineering and cyber security”. In *INTED2017 Proceedings* (2017): 4204-4211.

7. Wenke Lee and Bo Rotoloni. “Emerging cyber threats, trends and technologies”. Technical report, Institute for Information Security and Privacy (2016).

8. Social-engineer toolkit” (2022).

9. Kali Linux (2022).

10. Hadnagy. “Social engineering: The art of human hacking, Wiley (2011).