Social Engineering Attacks on the Cyber-Physical System: Human Cyber and Physical Impacts*

Robert Makila Beni(✉)

Université Nouveaux Horizons, Lubumbashi Route Kasapa 2465, Democratic Republic of the Congo
robert.makila@unhorizons.org

Abstract. Technological advancements have created new issues in IT security. Cyber-physical infrastructures, which mix physical elements with interconnected IT systems, have emerged as a major trend in industries such as transportation, energy, health, and public safety. However, the integration of the physical and digital worlds has generated new security threats, including social engineering attacks. Cybercriminals employ social engineering to trick users and obtain personal information or access privileges to computer systems. Social engineering attacks are frequently carried out using communication channels such as social networks, e-mails, and phone conversations. This study intends to investigate how social engineering attacks can be carried out in a cyber-physical-human environment. We will investigate the impact of cyber-physical-human infrastructures, cybercriminals' attack strategies, the effects of these attacks, and measures of prevention. The significance of this research stems from the fact that cyber-physical infrastructures are increasingly being employed in crucial scenarios where a breach in security could have fatal implications. It is therefore critical to understand the dangers associated with these infrastructures and to put adequate safeguards in place to protect them against social engineering attacks.

Keywords: Social Engineering · Cybersecurity · Cyber-physical Systems · Cyber-Physical-Human Systems · Human Factor · Industrial control systems

1 Introduction

Cyber-physical system (CPS) social engineering attacks are a rising worry. In order to get unauthorized access to sensitive data or systems, these assaults take advantage of human nature. Social engineering techniques can be used to persuade individuals to divulge private information, download malicious software,

* Université Nouveaux Horizons.

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 296–311, 2025.
https://doi.org/10.1007/978-3-031-81570-6_20

or access dangerous websites, all of which can jeopardize the security of CPS. Attackers frequently try to stop or slow down information flow, add unauthorized modifications to instructions or commands, send false information about how a system is operating, change ICS software and configuration settings, interfere with the operation of equipment protection systems, and also with the operation of safety systems.

The word has faced multiple malware attacks affecting industries with significant impacts : 1.In 1988, a Password attack on a programmable logic controller, causing a denial of service in the manufacturing plant, years after civil nuclear, chemical, energy, transport, water, food and health sectors also were targeted [3]. 2.The maroochy water services attack, causing a release of 265.000 gallons of untreated sewage [10]. 3.In 2016, an attack occured on ukrainian power grids, 30 stations were attacked depriving electricity to approximately 225.000 customers [10]. 4.The Pipedream recently launched in 2022, a disruptive and devastating attacks mutilple vital industrial devices [15]. Social engineering exploiting the human vulnerabilities is the reason thinking of the scenario on cyber-physcal infrastructures where he is an actor.

2 Related Studies

2.1 Human Factor, Cyber Hygiene, Cyber-Physical Systems, and Industrial Control Systems in the Context of Cybersecurity Master's Thesis Master of Engineering Cybersecurity 2023 , South-Eastern Finland University of Applied Sciences

This study investigates the cybersecurity risks of vital infrastructure systems, including human factors and operational technology (OT). The study proposes that the risk of cyberattacks can be mitigated by active learning, best practices, cultural change, fatigue and stress management, insider threat prevention, knowledge and skills development, personal safety, societal safety, and safety management [20].

The study also identifies the following OT best practices for reducing cyberattacks: Create and enforce a cyber hygiene policy - Implement cybersecurity awareness campaigns for employees and top management - Employ strict security policies - Implement an intrusion prevention and detection system (IPS/IDS) - Manage and control authorization and user accounts - Segment networks - Discover, identify, classify, and prioritize OT assets -Prevent OT threats - Implement physical security measures - Provide end-user awareness and training - Remove, disable, and rename unnecessary OT assets - Restrict the roles of temporary personnel -Secure remote access - Secure physical access - Keep software up to date, including operating systems, applications, and firmware - Use a web application firewall (WAF) - Implement virtual patch management. The study also recommends that CPS/ICS staff participate in cyber-exercises, such as penetration tests, phishing drills, ransomware drills, malware drills, DDoS drills, and

incident response drills. These exercises can help staff to learn how to cooperate and communicate effectively during a cyberattack, investigate attacks, and recover from attacks [20].

2.2 Looking Back to Look Forward: Lessons Learnt from Cyber-Attacks on Industrial Control Systems

There has been a variety of cyberattacks since the 1980 s that target industrial control systems (ICS), some of which have had an effect on parts of critical national infrastructure (CNI) [21].

Although there are restrictions on who can access information on ICS-focused hacks, especially in a CNI context, this paper gives a thorough summary of those that have been publicly disclosed. In order to better understand attack vectors, threat actors, impact, and targeted sectors and locations, cyber-security practitioners can identify and analyze previous ICS-focused cyberattacks. This is important for the ongoing creation of comprehensive risk management strategies [21].

2.3 A History of Cyber Incidents and Threats Involving Industrial Control Systems

Malicious cyber attackers have been focusing on industrial control systems that oversee vital infrastructure assets for a long time. The majority of these incidents don't receive as much media attention as those involving enterprise (information technology) systems, therefore neither their specifics nor the dangers they pose are as well understood [10].

An examination of publicly documented cyber events involving vital infrastructure assets is provided in this chapter. The occurrences listed below are by no means all of them. However, the report highlights the rising trends in the volume and complexity of cyberattacks and offers useful insights into the dangers and vulnerabilities facing industrial control systems [10].

2.4 Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents

Modern Information Technology (IT) components are being actively incorporated into industrial enterprises' critical infrastructures and their rigid Operational Technology (OT) architectures. However, as OT systems gradually grow more interconnected, they have subtly changed into enticing targets for various adversarial forces. This study presents a comprehensive and current survey of the most common threats and assaults against critical infrastructures, including Industrial Control Systems, as well as the communication protocols and devices used in these contexts [22].

This study shows that assaults on critical infrastructure increase in frequency due to the proliferation of cheap tools and methods that can help either the

early or late stages of an attack. Furthermore, the investigation reveals that certain OT-specific network protocols and devices have flaws in their design and execution that might easily allow adversaries to have a decisive impact on physical operations [22].

- The authors provide a thorough study and discussion of the significant ICS and critical infrastructure (CI) security incidents to date. This makes it possible to get a full picture of the strategies, tactics, and practices used by the attackers. The events are further classified based on the types of vulnerabilities that take advantage of the level of the ICS that is affected, their results, and potential mitigation techniques [22].
- A comparison of all popular communication protocols used in the context of ICS and CI with regard to security features. This talk also goes into detail about the flaws in protocols that have been identified by the pertinent literature, which leads to frequent attack types and significant obstacles to achieving a higher level of security.
- An examination and discussion of the flaws found in academic research on ICS-specific devices, as well as how these flaws are used to subvert CI and ICS control mechanisms [22].

3 Literature Review

3.1 Social Engineering

Social engineering is a non-technical attack that uses human interaction to deceive victims into disclosing personal information or acting in ways that are harmful to themselves or an organization [2].

The direct communication between the perpetrator and the victim is the foundation of social engineering. Instead of using brute force, the attacker will typically attempt to persuade the target to compromise themselves.. The attack cycle gives these criminals a constant way to deceive you [6,7].

Social Engineering Attack Cycle:

1. *Preparation.* The attacker will conduct background research on you or a larger organization in which you are connected. This data can be obtained through a variety of means, including social media, public records, and direct observation [2,5].
2. *Infiltration.* The attacker will cultivate trust before establishing a relationship or initiating an engagement. Email, phone calls, and in-person meetings can all be used to do this [2].
3. *Exploitation.* Once trust and a vulnerability have been created, the attacker will use the victim to further the attack. This can be accomplished by asking sensitive information, installing malware, or enticing the victim to engage in other dangerous behavior [2].
4. *Disengagement.* The assailant abruptly ceases contact with the victim following his malicious activity and vanishes [2].

Types of Social Engineering Attacks:

1. *Phishing.* is a sort of cyber attack in which the adversary sends an email or text message that looks to be from a genuine source [1,2], such as a bank or credit card firm. The email or text message will frequently include a link that, when clicked, would redirect the victim to a false website that appears to be the actual one. The attacker can take the victim's personal information if they enter it on the bogus website [5,7]
2. *Vishing.* also known as voice phishing, the victim is duped into providing sensitive information over the phone by using emotions and fear [6].
3. *Smishing.* also known as SMS phishing, the victim is duped into supplying personal information over SMS [6].
4. *Baitware.* is a sort of attack in which the attacker leaves a USB drive or other electronic device in a public location. When the victim plugs in the device, malware is frequently installed on their computer [2,5].
5. *Tailgating.* An attack in which the attacker accompanies a legitimate employee into a secure location. Once inside, the attacker has the ability to steal sensitive data or install malware [2,5].
6. *Pretexting.* is the act of impersonating someone in order to obtain information that will permit access. Pretexting is a form of social engineering attack in which the attacker fabricates a fake situation to acquire the victim's trust. For example, the attacker could impersonate a government official or a representative of a respectable organization in order to deceive the victim into disclosing sensitive information [2,6].
7. *Dumpster Diving.* is the process of searching for information in someone else's waste [2,5].
8. *Eavesdropping.* an attacker listens or reads a conversation without authorization; he can also intercept any type of communication [1,2].
9. *Reverse Social Engineering.* the attacker makes himself so important that the victim seeks his advise before or after the attacker provides the information required [5].
10. *Piggybacking.* the purposeful or unintended facilitation of an authorized person [2].
11. *Shoulder sniffing.* He peers over someone's shoulder to obtain sensitive information such as a PIN or a password [2,5].

3.2 Cyber-Physical Systems

A cyber-physical infrastructure (CPI) is an integrated system that combines computation, networking, and physical processes. CPIs are becoming more popular because they provide a number of benefits, including increased efficiency, productivity, and safety.

Types of CPS:

– *Smart grids.* which utilize sensors and networking to monitor and control the flow of electricity [1].

- *Smart transportation systems.* Smart transportation systems monitor and control traffic flow using sensors and networking [1].
- *Smart buildings.* employ sensors and networking to monitor and control energy consumption, lighting, and other functions. [1]
- *Industrial control systems.* Industrial control systems monitor and control industrial processes through the use of sensors and networking [1].

Cyber-Physical Infrastructure Vulnerabilities:

- *Cyberattacks.* Cyberattacks have the potential to disrupt or disable CPIs [1]. For example, a cyberattacker could take control of a smart grid and trigger a power outage.
- *Physical attacks.* Physical attacks can be used to disrupt or deactivate CPIs as well [1]. An attacker, for example, could damage a smart transportation system by destroying its sensors or networking equipment [4].

Social Engineering Attacks on Cyber-Physical Systems: Social engineering attacks are a sort of attack that uses human interaction to deceive victims into disclosing personal information or acting in ways that are harmful to themselves or an organization [1]. As cyber-physical systems (CPS) become more interconnected and reliant on software and networks, they are increasingly being attacked by social engineering attacks.
Here are some examples of CPS social engineering attacks:

- *Attack 1.* In 2010, an attack known as "Stuxnet" damaged numerous nuclear installations in Iran. Hackers from the United States have recently carried out a number of cyber-attacks on Iran [9].
- *Attack 2.* Two examples of hacking ICS assaults that can be used to spy on individuals are DuQu and Flame. In 2012, Flame, for example, targeted and discovered numerous ICS networks in the Middle East. The primary purpose of this spyware was to obtain confidential information from businesses, such as addresses and keys inputted [9].
- *Attack 3.* An attacker hacked a computer at a water filtering plant in Pennsylvania (USA) and utilized it as its own spam and pirated software distribution systems [9].

CPS will become more vulnerable to social engineering attacks as they become more linked and reliant on software and networks. Organizations must be aware of the hazards of social engineering attacks and take precautions to defend themselves.

4 Materials and Methods

4.1 Case 1:

To assess the impact of the information technology agent's phishing awareness, a phishing assault test was carried out on June 24 at 12:41, specif-

ically targeting the network administrator of a corporation with cyber-physical infrastructures categorized as smart buildings. The attack was prepared using the knowbe4 phishing tool to pretend to be an Insider IT using the email address it@companyname.domain. With an inoffensive link leading to a 404 not found page, the content explicitly requested a password change owing to a suspected breach. A second email was also sent to the attacker, robert.makila@unhorizons.org, to preview and check the efficacy of the scenario and ensure that it was delivered (Fig. 1).

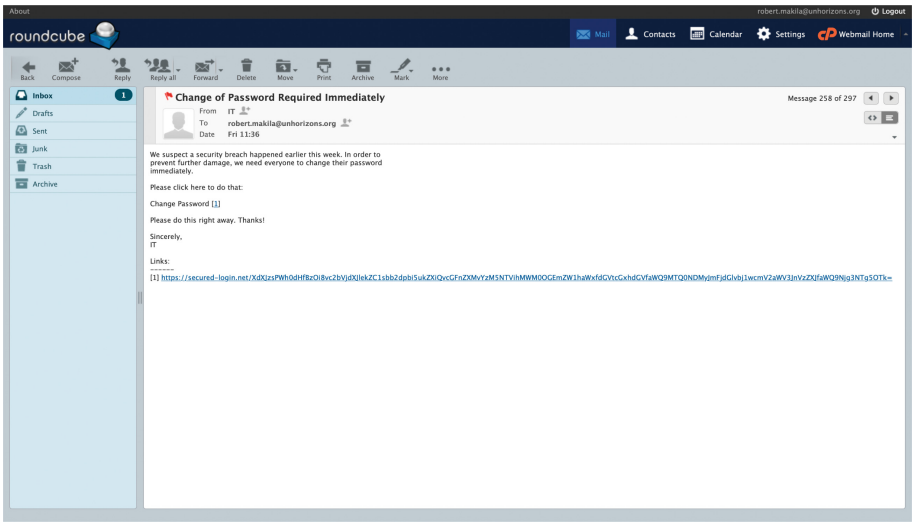

Fig. 1. Case 1 Phishing Attack Content.

4.2 Case 2:

Major CPS/ICS occurrences with a clearly defined attack history from 2000 to 2022 have been the subject of data collecting. A thorough examination of the first intrusion method to distribute or allow the malware to spread in the targeted systems is brought out from the historical narrative or scenario. Data is divided into two categories (cyber and physical) with the obvious purpose of determining the effect of social engineering approaches on cyber-physical systems. A strategy based on a cyber-physical-human assessment (Table 1).

The result demonstrates that ICS cyber attacks can be successful through a variety of delivery methods, including social engineering, insider attacks, and physical access. This suggests that a holistic approach to security is needed to mitigate ICS cyber attacks.

The Table 2 shows that social engineering, particularly spear-phishing, is the most common delivery method used in ICS cyber attacks apart from Directory

Table 1. Physical incidents table.

Ref	Name	Delivery Methods	Year
R [10]	Maroochy Water Service Breach	**Insider Attack**	2000
R [10]	Turkish Pipeline Explosion	**Physical access**	2008
R [10,11]	Stuxnet (Iran)	**Social Engineering : Tailgating, USB Stick**	2010
R [11,12]	Duqu	**Social Engineering : Tailgating, USB Stick**	2011
R [11–13]	Flame	**Social Engineering : Tailgating, USB Stick**	2011
R [3]	Shionogi	**Insider Attack**	2011
R [12]	Gauss	**Social Engineering : Tailgating, USB Stick**	2012
R [3]	Turbine control system	**Social Engineering : Tailgating, USB Stick**	2012
R [10,15]	Triton / Trisis	**Physical access**	2017

Table 2. Cyber incidents table.

Ref	Name	Delivery Methods	Year
R [10]	Night Dragon	**Social Engineering : Spear-Phishing**	2010
R [10]	Gas Pipeline	**Social Engineering : Spear-Phishing**	2012
R [10]	Shamoon	**Social Engineering : Spear-Phishing**	2012
R [3]	Niagara AX	**Directory Traversal**	2012
R [10]	Target Stores	**Social engineering : Phishing**	2013
R [10]	New York Dam	**Internet Accessible Device**	2013
R [10]	Havex	**Social engineering : Phishing**	2013
R [10,15]	German Steel Mill	**Social engineering : Spear-Phishing**	2014
R [10,15]	Dragonfly/Energetic Bear.1	**Social engineering : Spear-Phishing**	2014
R [10]	BlackEnergy	**Social engineering : Spear-Phishing**	2014
R [10,15]	Ukraine Power Grid1	**Social engineering : Spear-Phishing**	2015
R [10]	Kemuri Water Attack	**Vuln. on the Internet-facing payment App. server**	2016
R [10]	Shamoon 2	**Social engineering : Spear-Phishing**	2016
R [10]	Ukraine Power Grid2	**Social engineering : Spear-Phishing**	2016
R [10]	CRASHOVERRIDE / Industroyer	**Social engineering : Spear-Phishing**	2017
R [10]	APT33	**Social engineering : Spear-Phishing**	2017
R [10]	NotPetya	**Social engineering : Spear-Phishing**	2017
R [10]	Dragonfly/Energetic Bear.2	**Social engineering : Spear-Phishing**	2017
R [3]	Wolf Creek	**Social engineering : Phishing**	2017
R [19]	Samsam - Transportation	**Remote Desktop Protocol**	2018
R [18]	Norsk Hydro	**Social engineering : Spear-Phishing**	2019
R [3]	Oil producers attack	**Social engineering : Spear-Phishing**	2020
R [3]	Israeli Water Facilities	**Internet Accessible Device**	2020
R [3]	Honda	**Social engineering : Spear-Phishing**	2020
R [16]	Florida wanter plant attack	**Watering Hole**	2021
R [17]	Kojima industries attack	**Social engineering : Spear-Phishing**	2022
R [15]	Pipedream	**Social engineering : Spear-Phishing**	2022

traversal, Internet accessible device, phishing, watering hole and remote desktop. This is because spear-phishing attacks are targeted and personalized, making them more likely to be successful (Table 3).

5 Data Analysis and Results

5.1 Case 1:

Table 3. Case 1 Result table.

Target	Action	Time
Network Admin	Click	**Within the first 8 h of the attack**

The network administrator clicked on the simulated malicious link within the first 8 h of the attack, the attacker could gain access to the network and launch further attacks. The network administrator could then be used to spread malware to other devices on the network, steal sensitive data, or disrupt operations.

The human in a cyber-physical system can also make use of social engineering concepts as an insider. Insider attacker knows the infrastructure , can be able to not trigger the IDS alert, is trusted because he belongs to the targeted workers of the organization.

someone that has knowledge of the organization's information and intentionally negatively impacts the enterprise's integrity. In most cases, malicious insiders are former employees, contractors, or business partners, employees that never follow the information technology procedures and rules. employee whose computer is infected with malware. The attacker in the similar way of insider, used the insider email schema to build trust with the victim (Fig. 2 and 3).

5.2 Case 2:

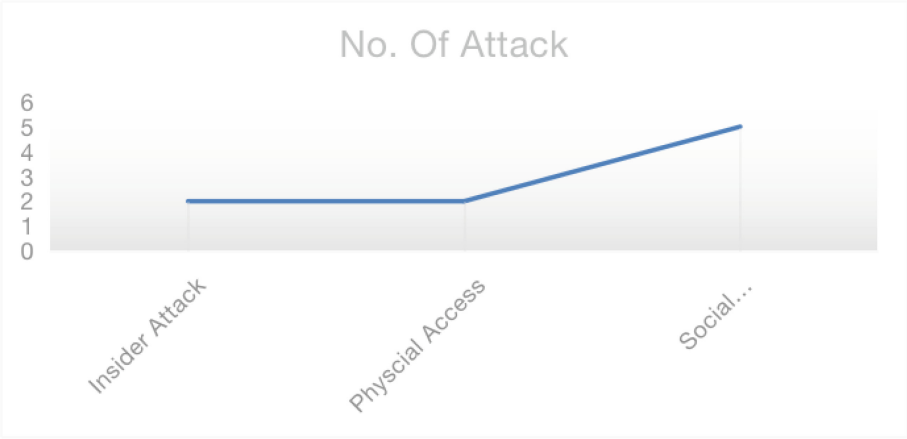

Fig. 2. Physical Incidents Result

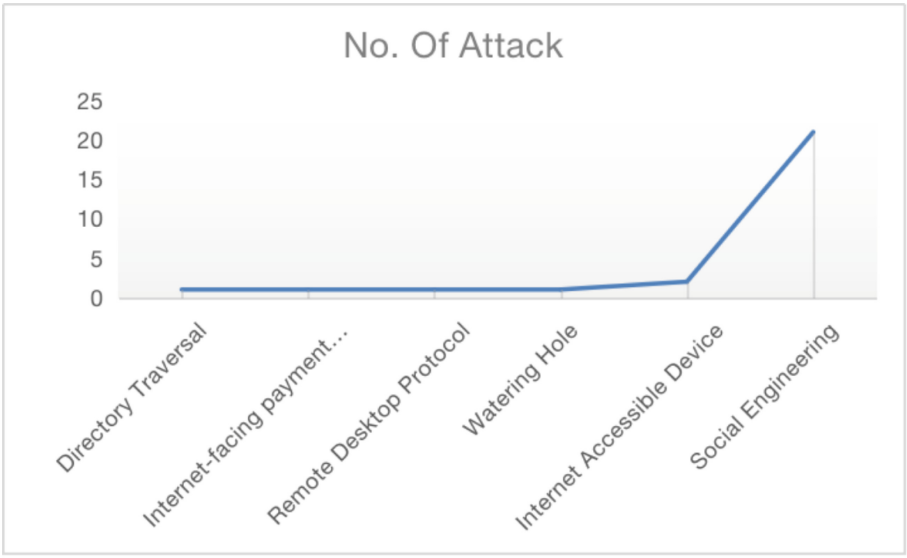

Fig. 3. Cyber Incidents Result

6 Discussion

6.1 Cyber and Physical Impact

Case 1 :
Targeting the Network Administrator is an attack with significant impact, as long as he stores very sensible information of the IT infrastructure (Password, etc.).

The attacker employed social engineering attack techniques to make the attack successful by appealing to the IT Administrator's emotions by posing an urgent scenario and requesting that he changes the password due to a security breach. In order to make the victim accept the pretext and think the source was an insider, the attacker also employed impersonation when sending the email with a reliable email account (the same domain name with the victim).The victim was unable to think whether or not to click the link . A phishing attack, which has been demonstrated in this study to be destructive on getting access to the internal network and the hacker can change data, break the confidentiality and integrity of the system after having access to the system.

Case 2 :
After gathering major incidents in the cyber-physical systems from 2000 to 2022, with a clear history of what exactly happened. One aspect and difficulty of conducting this study is that certain attacks remain unclear in their history, some companies hide information or deny attacks. we have been able to distinguish

cyber and physical incidents based on the prior delivery method used to conduct the attack. And results are significant in terms of social engineering attack aspects. The weakest component of the cyber-physical systems is the human. The reason that attackers used social engineering attacks in order to deliver malicious code or malware into the victim's system. This investigation has found the following results (Table 4):

Types of attacks :

- Physical attacks 25 %,
- Cyber attacks 75 % ;

Mode of attack : Social engineering :

- Physical attacks 55.5 %,
- Cyber Attacks 77.7 %,
- Cyber-Physical 58.3 %;

Average attack :

- Physical attacks 3 ,
- Cyber attacks 4.5.

Table 4. Cyber and Physical Impact table.

Statistics	Attack	Success rate
Rates : Physical attack	Physical	**25%**
Rates : Cyber attack	Cyber	**75%**
Mode : Physical attack	Social Engineering	**55.5%**
Mode : Cyber Attack	Social Engineering	**77.7%**
Mode : Cyber-Physical	Social Engineering	**58.3%**
Average : Physical Attack	Physical	**3**
Average : Cyber Attack	Cyber	**4,5**

Social engineering is the most common mode of attack for all these two types of attacks (Fig. 4 and (Table 5)).

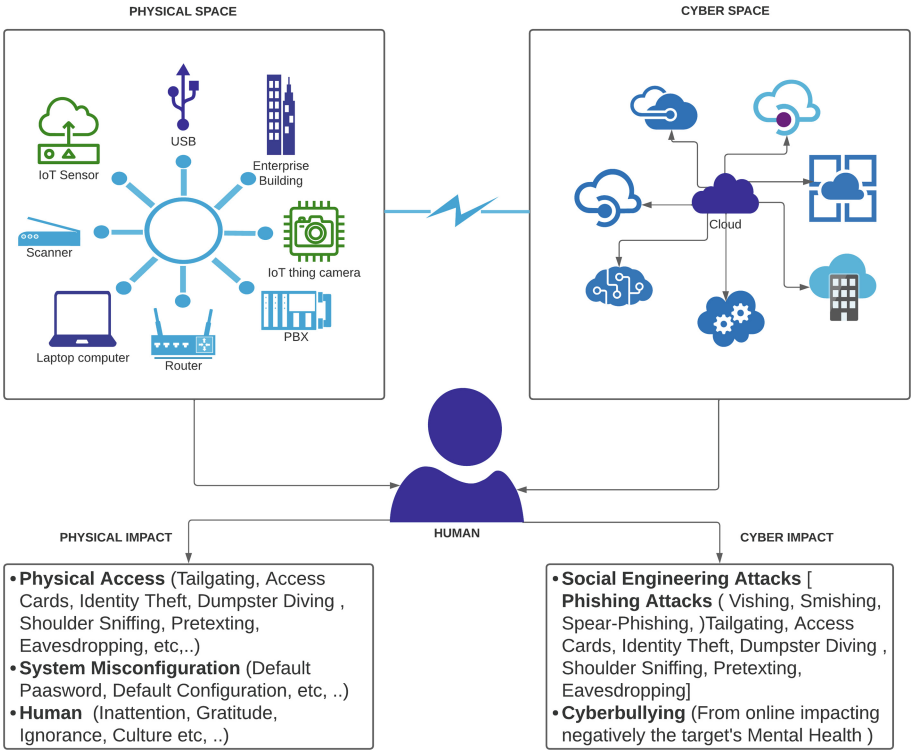

Fig. 4. Cyber and Physical Impact.

Table 5. Social Engineering : Cyber and Physical Impact with security goals table.

Attacks	Security goals affected	Cyber Impact	Physical Impact
Phishing, Vishing, Smishing, Spear Phishing, etc. ..	**Confidentiality, Integrity, Availability, Authentication**	- Malicious Injection - Sensitive Data Manipulation - Disclosure of sensitive information such as passwords, credits card number, - Malware Installation - Abuse of privilege	- Device dysfunction - Data loss integrity - Financial loss - Loss of reputation - Loss of production and revenue.
Pretexting, Impersonation, Tailgating, Diversion Theft, Baiting, Piggybacking, Reverse social engineering, etc. ...	**Confidentiality, Integrity, Availability**	- System disruption - Unauthorized Access. - Malware Installation	- Corporate espionage -Identity theft - Data Leakage - Trade secret disclosure
Eavesdropping	**Confidentiality**	- Information disclosed such as Password, Digital Signature	- Information disclosed such as physical address, reports, financial statement, Decision reports.
Shoulder Sniffing	**Confidentiality**	- Password, sensitive information are taken	- Important documents, evidence, information are disclosed

6.2 Social Engineering : Cyber and Physical Impact with Security Goals

6.3 Impact on Human and Good Security

Data Breaches. Social engineering attacks can be used to get sensitive data, such as consumer information, employee information, or intellectual property. This information can then be utilized for harmful objectives like identity theft, fraud, or industrial espionage [5,8].

Disruptions to Critical Systems. Social engineering attacks can be used to disrupt critical systems such as electricity grids, transportation systems, or water systems. This can result in fatalities, property destruction, and economic upheaval [8].

Physical Harm. In some circumstances, social engineering attacks can cause physical harm to someone. An attacker, for example, could employ social engineering to deceive someone into opening a door or entering a building, where they could be attacked [4,9].

Loss of Trust. Successful social engineering attacks can destroy trust between individuals, organizations, and governments. This can make collaboration on critical problems like cybersecurity and national security more challenging [9].

6.4 Consequences on Economics and Politics

Social engineering attacks can also have a huge economic and political impact. A data breach, for example, could cause a loss of trust in a firm or organization, resulting in a drop in sales or investment. A system outage could result in economic consequences such as lost production or infrastructure damage [9]. A physical attack could also result in the loss of life or major property damage, both of which could have a huge impact on a community or region [7,9].

Economic Losses. Social engineering attacks can result in economic losses such as lost productivity, infrastructure damage, and reduced investment [7,9].

Political Instability. Discord and instability within a country or region can be sown via social engineering attacks. This can make achieving political goals like peace and prosperity more challenging [7,9].

7 Measures for Prevention

Employee Education. Employees should be taught how to recognize and report suspicious emails and phone calls . They should also understand the dangers of social engineering attacks and how to defend themselves. Being cautious with the information disclosed online, particularly on social media, to suspicious emails, imposters, phishing, etc. ... [5]

Security Measures. such as firewalls, intrusion detection systems, updating programs with the most recent security updates, using strong passwords [5], update them on a frequent basis and data encryption, can aid in the protection of cyber-physical systems against social engineering attempts [4,8].

Maintaining Resilience. Cyber-physical systems should be built to withstand social engineering attacks. This can be accomplished by employing redundant systems and situating essential systems in secure regions [5,8].

The novel approach to mitigating CPS cyber attacks based on human, cyber and physical aspects that have been outlined addresses all three of these delivery methods. By implementing a comprehensive security program that includes also Background checks, Firewalls, Intrusion detection and response systems, Encryption, Access Control and video surveillance and Physical barriers can significantly reduce the risk of a successful CPS cyber attack.

8 Limits and Perspectives Research on Social Engineering Attacks on Cyber-Physical Systems

There are several limitations to study on CPS social engineering attacks. One limitation is that replicating real-world attacks in a laboratory setting might be challenging. This work is crucial for the development of appropriate security mechanisms to safeguard CPS from these threats.

Understanding the Psychology of Social Engineering. what makes people vulnerable to social engineering attacks and how to develop effective responses.

Improving Security Awareness. attempting to increase CPS users' security awareness so that they can better identify and resist social engineering attempts.

The study of social engineering attacks on CPS is still in its early phases, but it is a significant area of study that has the potential to enhance CPS security.

9 Conclusion

Social engineering is a non-technical attack that uses human interaction to deceive victims into disclosing personal information or acting in ways that are harmful to themselves or an organization. As cyber-physical systems (CPS) become more interconnected and reliant on software and networks, they are increasingly being attacked by social engineering attacks. The basic notion behind social engineering on CPS is to use the human factor to obtain access to or control of a CPS. This can be accomplished through several strategies such as phishing, tailgating, and pretexting.

References

1. Jean-Paul, A.Y., Ola, S., Hassan, N.N., Nesrine, K., Ali, C., Mohamad, M.: Cyber-physical systems security: limitations, issues and future trends. Microprocessors Microsyst. **77**(103201), 1–15 (2020)
2. Breda, F., Barbosa, H., Morais, T.: Social engineering and cyber security. In: 11th International Technology. Education and Development Conference on Proceedings, pp. 4204–4211. IATED, Valencia, Spain (2017)

3. Thomas, M., Alexander, S., Sam, M., Miriam, S., Benjamin, G.: Looking back to look forward: lessons learnt from cyber-attacks on industrial control systems. Int. J. Crit. Infrastruct. Prot. **35**(100464), 1–18 (2021)
4. Solange G,.: Cybersecurite , Securite Informatique et Reseaux. 5th edn. Dunod, France (2016)
5. AqibHafiz, R.S., Jyoti.: social engineering attacks and prevention: a mirror review. Think India J. **22**(16), 2530–2536 (2019)
6. Ansh, M., Dev, V., Harsh, S., Jay, K., Dharmil, G.: A review of social engineering attacks and their mitigation solutions. Int. J. Eng. Tech. Res. **10**(10), 215–220 (2021)
7. Al-Mhiqani, M.N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z.Z., Ali, N.S., Abdulkareem, K.H., : Cyber-security incidents: a review cases in cyber-physical systems. Int. J. Adv. Comput. Sci. Appl. **9**(1), 500–508 (2018)
8. Ajeet S. , Anurag J.: Study of cyber attacks on cyber-physical system. In: 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT) on Proceedings, pp. 686–690. Elsevier, Jaipur (India) (2018)
9. Amit, K., Sreenath, N.: Cyber physical systems: analyses, challenges and possible solutions. Internet Things Cyber-Phys. Syst. **1**, 22–33 (2021)
10. Hemsley, K., Fisher, R.: A history of cyber incidents and threats involving industrial control systems. In: ICCIP 2018. IAICT, vol. 542, pp. 215–242. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-04537-1_12
11. Eric, D.K., Joel, T.: Industrial Network Security (Second Edition), Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2nd edn. Syngress-Elsevier, USA (2014)
12. Paulo, S., Jana, S., Andrew, R.: Introduction to Cyber-Warfare: A Multidisciplinary Approach. Elsevier, USA (2013)
13. Rosenberg, J.: Embedded security, Rugged Embedded Systems: Computing in Harsh Environments. Elsevier, USA (2017)
14. Fayi, S.Y.A.: What Petya/NotPetya ransomware is and what its remidiations are. In: Latifi, S. (ed.) Information Technology - New Generations. AISC, vol. 738, pp. 93–100. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-77028-4_15
15. Malik, M.I., Ibrahim, A., Hannay, P., Sikos, L.P.: Developing resilient cyber-physical systems : a review of state-of-the-art malware detection approaches, gaps, and future directions. Computers **12**(4), 79,1–26 (2023)
16. Few, C., Thompson, j., Awuson-David, K., Al-Hadhrami, T.: A case study in the use of attack graphs for predicting the security of cyber-physical systems. In: 2021 International Congress of Advanced Technology and Engineering (ICOTEN) on Proceedings, pp. 1–7. IEEE, Yemen (2021)
17. Md, H.R., Thorsten, W., Mohammed, S.: Manufacturing cybersecurity threat attributes and countermeasures: review, meta-taxonomy, and use cases of cyber-attack taxonomies. J. Manuf. Syst. **68**, 196–208 (2023)
18. Oueslati, N.E., Mrabet, H., Jemai, A., Alhomoud, A.: Comparative study of the common cyber-physical attacks in industry 4.0. In: 2019 International Conference on Internet of Things. Embedded Systems and Communications (IINTEC) on Proceedings, pp. 1–7. IEEE, Tunis, Tunisia (2019)
19. Hasssan, N.: Ransomware Revealed. Apress, Berkeley (2019)
20. Tuomala V.: Human factor, cyber hygiene,cyber-physical systems, and industrial control systems in the context of cybersecurity. Master thesis, South-Eastern Finland University of Applied Sciences, pp. 1–92 (2023)

21. Miller, T., Staves, A., Maesschalck, S., Sturdee, M., Green, B.: Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. Int. J. Crit. Infrastruct. Prot. **35**(100464), 1–19 (2021)
22. Makrakis, G.M., Kolias, C., Kambourakis, G., Rieger, C., Benjamin, J.: Industrial and critical infrastructure security: technical analysis of real-life security incidents. IEEE Access **9**, 165295–165325 (2021)