Enhancement of Phishing Email Detection with Bayesian Networks: A Cyber Security Training Module

Dimitrios Lappas[1], Panagiotis Karampelas[2] and Giorgos Fesakis[1]
[1]University of the Aegean, Rhodes, Greece
[2]Hellenic Air Force Academy, Dekeleia, Greece

dlappas.aegean@gmail.com
panagiotis.karampelas@hafa.haf.gr
gfesakis@rhodes.aegean.gr

Abstract: In today's digital world, we rely on various applications to protect ourselves from malicious software on the internet. Many of these tools also aim to shield us from phishing emails, which are increasingly prevalent. But how reliable are these phishing protection tools? Do we uncritically trust their indication that an email is safe, or are their assessments merely probabilistic estimates? These questions became the focal point of an innovative educational process in cybersecurity training. In this training activity, participants initially assumed the role of phishing email creators, crafting emails targeting a hypothetical individual using social engineering techniques introduced during the course. Next, an anti-phishing software tool, developed specifically for this training, evaluated their emails and provided a percentage indicating the likelihood that the email would be identified as phishing. The software's functionality was built upon a Bayesian network designed specifically for the course, using data derived from emails created by participants in the previous academic year. Trainees were then introduced to Bayes' rule and learned how the Bayesian framework operates as a method of phishing detection. By the end of the training intervention, participants were proficient in applying Bayes' rule and constructing small Bayesian networks to assess the potential risk of emails, thereby enhancing their understanding of cybersecurity principles and tools. Our module makes a significant contribution to the cybersecurity education community by presenting an innovative approach to teaching protection against phishing emails.

Keywords: Phishing, Anti-Phishing, Bayes rule, Bayesian networks, Cyber teaching module

1. Introduction

A common experience for internet users is receiving warnings from various applications about potential malware on websites they attempt to visit. Typically, these warnings do not confirm the presence of malicious software with certainty; rather, they alert the user to the possibility of fraud. In this context of uncertainty, the user must ultimately decide whether to proceed to the site or not. Additionally, many applications warn users about potential attempts to intercept personal data related to financial transactions — such as usernames and credit card passwords — a technique known as phishing.

Phishing remains the most prevalent form of cybercrime, with approximately 3.4 billion spam emails sent daily (phishing statistics 2024). These attacks exploit human error, relying on moments when individuals overlook, or disregard established email safety protocols. While most users adhere to email hygiene and safe usage practices, statistics reveal a small but persistent proportion who fall prey to such schemes (phishing statistics 2024). Phishers typically aim to deceive their targets into divulging sensitive, financially valuable information, carefully selecting their victims to maximize potential gains.

A method frequently employed by phishing detection applications is the use of Bayesian Networks (Wang et al., 2020; Seryasat, 2021). A Bayesian network is a probabilistic graphical model that measures the conditional dependence structure of a set of random variables and leads to useful conclusions (Jensen, 1996). In cybersecurity, Bayesian networks are used to model and analyze network vulnerabilities, predict potential threats, and determine the likelihood of security breaches (Mokhtarian et al., 2022).

Inspired by the ability of Bayesian networks to predict potential phishing emails, we developed a novel teaching methodology for introducing anti-phishing awareness and protection. Our educational activity was designed within a scenario-based learning framework and consisted of five stages: Lecture – phishing theory, Practice – phishing email construction, Trigger – check the emails using a Bayesian Network, Lecture – analysis how the Bayesian Network works, Practice – anti phishing exercises from trainees.

Our approach to teaching Bayes' theory on the base of anti-phishing protection is innovative because it offers:

- Realism: Both the learning objectives and the simulation environment align closely with real-world scenarios, going beyond simple replication to create authentic experiences.

- Challenge for Learners: By evaluating emails created by their peers, students are actively engaged and motivated to participate in the Bayes theory learning process.
- Student Choice: Each student can select thematic areas for developing phishing emails, allowing them to tailor their learning experience and engage with content that interests them.
- Active Participation: Students begin by constructing their own phishing emails, then interact with the detection software specifically designed for this educational exercise. Through this interaction, they gain insight into how Bayesian networks function, effectively building new knowledge through hands-on experience.
- 360-degree approach: Students assume both the role of attacker (phisher) by exploiting the profile of the hypothetical victim and the role of the victim who uses advanced artificial intelligence tools based on Bayes network to detect phishing emails.

The module aims to equip participants with practical skills and theoretical knowledge to address phishing threats and cybersecurity challenges. At the end of the module, participants were able to:

- Diagnose phishing email attacks using attractive context: Recognize and identify phishing attempts in email communications.
- Apply critical thinking and problem-solving skills in anti-phishing efforts: Detect both current and future phishing-based attacks on computer systems and networks.
- Utilize Bayesian networks: Analyze and interpret previous data to support decision-making and problem-solving in an information security environment.

Our paper makes a significant contribution to the cybersecurity education community by presenting an innovative approach to teaching protection against phishing emails. By integrating theory with hands-on practice, we successfully captured trainees' interest while fostering an experiential learning environment. The uniqueness of our methodology lies in its dual-role perspective: trainees first assumed the role of attackers, crafting phishing emails, and later transitioned to the role of defenders, analyzing and predicting the likelihood of an email being phishing. This comprehensive, immersive approach can be aptly described as a 360-degree methodology in cybersecurity education.

The paper is organized as follows: the second part presents the theoretical framework, defining the concept of phishing and Bayesian networks. Additionally, it examines scenario-based learning, concluding with the author's decision to work with this method. The third part details the steps of the module and the paper ends with the conclusions in part V.

2. Theoretical Part

2.1 Phishing – Anti-Phishing

2.1.1 Phishing detection techniques

Phishing attacks exploit vulnerabilities arising from human error, often targeting weaknesses in end users, who are considered the weakest link in the security chain. This widespread problem lacks a universal solution, necessitating the use of multiple techniques to address specific vulnerabilities and mitigate various types of attacks effectively. The four main approaches for detecting email phishing are (Khonji et al., 2013): (a) detection through blacklists, (b) detection using heuristic methods, (c) detection based on visual similarity, and (d) detection employing machine learning techniques.

With the rapid advancement of Artificial Intelligence, machine learning has become a cornerstone of modern email phishing detection techniques. Its integration into phishing detection marked a transformative shift in research, enabling systems to analyze and identify phishing attempts with unprecedented accuracy and efficiency. Initial efforts focused on leveraging supervised learning algorithms, including decision trees, random forests, and support vector machines, to classify phishing messages. These classifications were based on features extracted from email content, metadata, and URLs (Chen et al., 2017).

Relying solely on technical solutions for phishing detection is insufficient, as users often fall victim to attacks that leverage impersonation tactics designed to appear credible (Williams et al., 2017; Yang et al., 2017). Phishing attacks, a form of social engineering, exploit human error or psychological vulnerabilities to extract sensitive information (Dunham, 2004; Williams et al., 2017). These attacks typically unfold in three stages: delivering the phishing attempt to the target, the target's willingness to engage with the phishing content, and the subsequent

use of the illegally obtained data (Tandale & Pawar, 2020). To address these risks, many security experts advocate for anti-phishing awareness as a complementary measure, which is explored in the next section.

2.1.2 Anti – phishing awareness and training

Despite advancements in technical solutions, a significant number of information security breaches persist, many of which could be avoided with greater focus on human behavior (Hart et al., 2020). While security systems provide increasingly sophisticated defenses—such as detecting anomalies in data movement—their effectiveness diminishes when users fail to adhere to established security protocols (Torten et al., 2018). This highlights the critical role of human factors in ensuring the success of technological safeguards. Thus, training techniques that aim to cultivate users' awareness are vital in coping with phishing. As in the case of phishing detection techniques, there are also different approaches in anti-phishing awareness training. Anti-phishing training usually appears in two forms: (a) simulation-based training and (b) game-based training.

Simulation-based anti-phishing training typically involves immersing users in a virtual business environment where they receive simulated emails and determine whether these emails are legitimate or phishing attempts (Jagatic et al., 2007). In contrast, game-based training introduces a more interactive element, requiring trainees to identify phishing characteristics, such as suspicious URLs or email addresses, through gameplay. Some game-based approaches even challenge participants to create a malicious link that could be used in a phishing email, thereby deepening their understanding of phishing tactics from an attacker's perspective (Vayansky et al., 2018).

For a more comprehensive approach to phishing email training, we advocate for learners to first adopt the role of an attacker by crafting phishing emails. This perspective allows them to gain deeper insight into the tactics and characteristics that define suspicious emails, thereby enhancing their ability to identify them. Moreover, given that protection software is not entirely foolproof, understanding its operation experientially fosters a critical awareness of its limitations. This dual perspective not only prevents overreliance on automated solutions but also encourages vigilance in recognizing phishing attempts. These considerations formed the foundation of our decision to develop this specialized educational application.

2.2 Bayes Theory

2.2.1 Bayes rule and Bayesian networks

According to Bayes' theorem, if we know a conditional probability, let's say P(B|A), then we can calculate the inverse with the following formula:

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}$$

The importance of Bayes rule is that probabilities are considered to be expressions of subjective beliefs, meaning that they can be updated with new data. Bayes' rule is central to Bayesian inference, which is the use of probabilities to express our uncertainty about parameter values after observing data. Observation and estimation are sufficient to draw any conclusions.

A Bayesian network is a graphical representation of a problem that leads to useful conclusions through a complex joint probability distribution (Jensen, 1996). The capabilities offered by Bayesian networks constitute a powerful tool in all areas where diagnosis, prediction and modeling of complex interactions under uncertainty are required (Khuda, 2021). With Bayes diagrams, emphasis is placed on the schematic representation of the relationships between various factors - data of a problematic situation as well as the results between their combination (Cooper & Herskovits, 1996). In addition, Bayesian networks offer a representation of the probabilistic structure of the systems being studied and may serve as a method for uncertainty modeling and prediction.

2.2.2 Constructing Bayesian networks through knowledge engineering

One method to build a Bayesian network is knowledge engineering, where the domain of a specific problem is studied to define qualitative elements such as direct relationships between variables (Garcia et al., 2005). These relationships form the network structure. When historical data exists, estimating probabilities is straightforward. However, in cases where prior data is unavailable, initial probabilities must be estimated, which can be based on observed frequencies from relevant educational activities or expert input. This approach allows for flexibility in modeling, enabling Bayesian networks to support decision-making across a wide range of fields.

2.2.3 Bayesian networks in phishing detection

Bayesian networks, with their capacity to predict and express uncertainty in percentage terms, have piqued the interest of experts, who began to explore their use in phishing email detection. Initial results were promising, showing Bayesian Networks' effectiveness in identifying phishing emails (Meyer & Whateley, 2004; Raj & Mittal, 2018). This led to the development of several related tools, including:

- A Bayesian Network-based anti-phishing toolbar designed to help users identify phishing websites and protect sensitive information (Tandale, & Pawar, 2020). Bayesian filters in this toolbar support phishing detection directly within the web browser.
- Bayesian networks applied to detect phishing emails by assessing similarity with pre-identified phishing emails, with the detection rate quantified as a percentage (Zhang et al., 2011).
- Bayesian text-based filtering used for suspicious emails (Eberhardt, 2015). This filter could adapt based on new data, allowing for changes in its accuracy.
- Bayesian Networks integrated into the Factor Analysis of Information Risk (FAIR) model, one of the leading frameworks for quantitative cybersecurity risk assessment (Wang et al., 2020).
- A machine learning approach employing a dataset to train Bayesian Networks in phishing website detection (Seryasat, 2021).

These advancements highlight the role of Bayesian Networks as effective tools in cybersecurity, offering probabilistic measures of risk and reliability in phishing detection and beyond. As can be seen Bayesian networks play a significant role in anti-phishing attempts and thus we endorsed the specific approach in our training activity.

2.3 Scenario Based Learning

2.3.1 Definitions and applications of scenario-based learning

Godet and Roubelat (1996) describe a scenario as a sequence of events enabling forward movement in time, while Wilkinson (1995) considers it a narrative of possible developments over time. Such narratives can stimulate theoretical reflection on future developments, encourage discussion, and ignite imagination. Nadolski et al. (2008) further explain that scenarios can mirror real-life situations, engaging learners in activities like decision-making, problem-solving, and advanced reasoning. Through scenario-based learning, students work within a narrative centered on a problematic situation they must resolve, allowing them to apply their knowledge, critical thinking, and problem-solving skills within a safe, realistic environment. This approach promotes deeper understanding, involving students in critical incidents that compel them to evaluate multiple factors, make decisions, and reflect on outcomes (Errington, 2010).

2.3.2 Role of scenarios in achieving learning objectives

Margetson (1998) suggests that scenarios help achieve learning goals in two main ways: by serving as a story model for organizing acquired knowledge or as a practical framework that deepens understanding. The main feature of "learning through scenarios" is that students engage in authentic, structured learning activities that guide them toward discovering relevant concepts and processes (Burden & Byrd, 2010). This sequential approach fosters heuristic experiences, helping students learn critical concepts through experience (Clark, 2009). For this purpose, we adopted the scenario-based approach as the suitable learning methodology for our approach.

3. Training Module for Phishing Email Protection

The module was held on December 2, 2024, at the Hellenic Air Force Academy as part of the "Cyber Warfare" training within the "European Union Military Erasmus" program. A total of 82 students from four different European countries, aged 19 to 21, participated in the training. All participants were cadets from military academies. The module spanned six training hours. Participants were provided with a worksheet containing questions to assess their understanding of the lesson. Additionally, they were required to calculate Bayesian probabilities for problems included in the worksheet. The phases of the module are illustrated in figure 1.

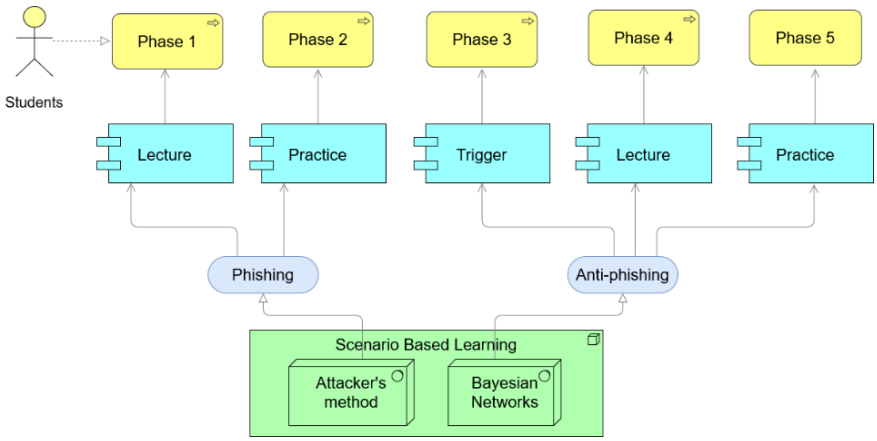

Figure 1: The training module for phishing email protection

- Phase 1: Trainees were introduced to the fundamentals of phishing, along with a template for crafting phishing emails.
- Phase 2: Participants created their own phishing emails within a designated hypothetical scenario.
- Phase 3: The phishing emails crafted by students were analysed using a custom-built application designed by the authors, which used previous data to identify potential phishing indicators within the scenario (based on a Bayesian Network).
- Phase 4: The results from the phishing detection application served as a practical segue into the analysis of Bayesian theory.
- Phase 5: Participants engaged in hands-on exercises to solve practical tasks related to Bayes' rule, reinforcing their learning through application.

3.1 3.1 Phase 1: Lecture About Phishing Emails Construction

The lecture started presenting to the participants the general characteristics of phishing emails and the role of social engineering in phishing email construction. Then, a method was presented describing the steps that the attackers may follow in order to persuade victims to click on a suspicious link in their email as described by Lappas and Karampelas (2023). In summary, the proposed methodology included the following steps:

- Step 1: Information gathering about the victim.
- Step 2: Grouping – categorization of the victim's information.
- Step 3: Evaluation of information - choose to use the category in which the victim expresses more liking or spends more time.
- Step 4: Search for dominant emotion or desires of the victim in the above category
- Step 5: Mapping the victim's contacts – friends who have the same interests.
- Step 6: Finding a real or imaginary entity (organization or person) that the victim could trust.
- Step 7: Finding a motive for the victim to follow the instructions included in the e-mail.
- Step 8: Views of experts.

After the presentation of the proposed methodology, trainees were asked to follow these steps and make a message of a spear phishing email for a hypothetical scenario described in the next paragraph.

3.2 Phase 2: Practice on Hypothetical Scenario

The scenario for practice included a hypothetical person who had a profile on a social media page. On this page, he posted details about his life including job, hobbies, family, friends and likes. More specifically, the hypothetical person was a German pilot of a fighter aircraft who loved running and he was very keen on the military history of aircrafts. He had special healthy diet preferences and he liked specific running shoes. He was also referring to many posts to a friend of him named Josh, to his daughter, to the places he had visited during his vacation and the kind of beers he likes to drink. Everyone could access his profile in the designated social media (Figure. 2).

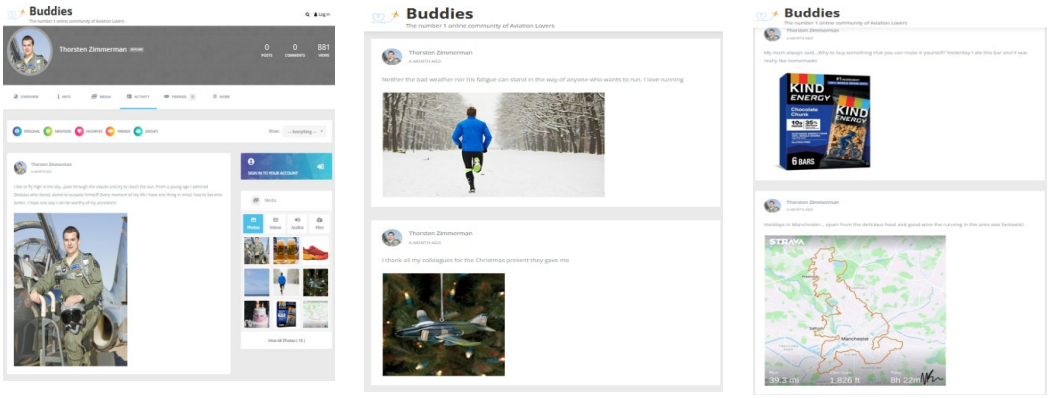

Figure 2: The fake profile that was used for the practice

Participants took the role of a social engineer. Their task was to create a phishing email. More specifically, they were asked to create the content of a phishing email and send it to this hypothetical person. The objective of the email was the victim to click on a hyperlink which automatically would download a malware in his device with the purpose of collecting confidential information. An example of the participants' emails is the following:

> *Dear Thorsten,*
>
> *We would like to offer a great opportunity.*
>
> *Your friend Josh gave us your email in order to tell you about the rising stock prices of "Kind Energy Bars". According to your friend, you love our products, and we would like to have you amongst our investors. As you know our products' selling are skyrocketing now and you can buy stocks on a very cheap price. JUST NOW our stocks is only 10$ per share. If you buy it now your profit will be 10x more tomorrow, BUT you need to hurry, because the price is only available now. Your future financials will be secured for your entire lifetime. Please manage your order here: URL …..*
>
> *"The most important investment you can make is in yourself" - Warren Buffett*
>
> *Sincerely, Kind Energy Team*

3.3 Phase 3: Check the Emails in Anti-Phishing Software

Participants were then invited to insert the text of their email from the previous phase in the anti-phishing tool we had constructed. The aim of this action was to get feedback from the protection software the potential victim it was supposed that he had. As a result, they received a percentage expressing the probability of their email being phishing (Figure.3).

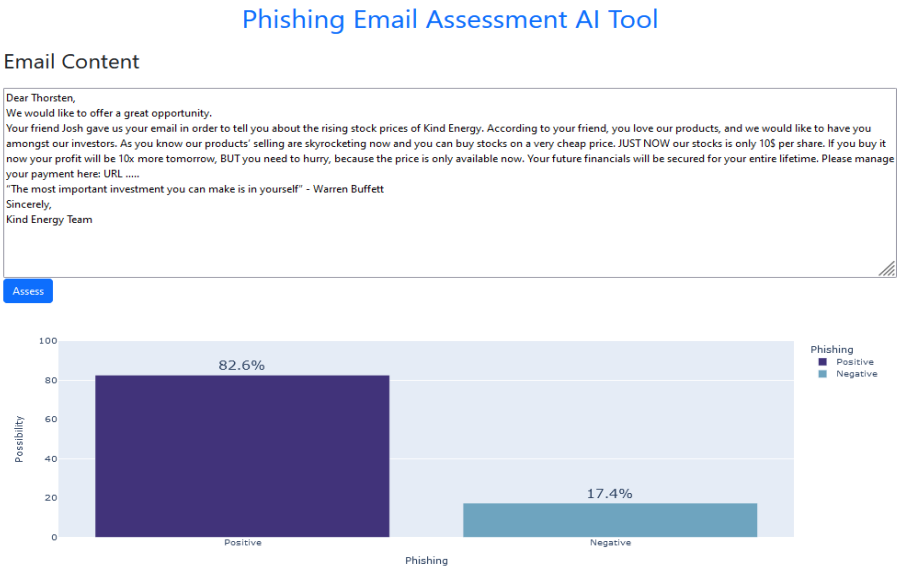

Figure 3: Checking an email in our AI tool

Students in general were impressed and puzzled by the results. A conversation among them in the auditorium was started about whose email had the lowest percentage. That was a tickler for the next phase.

3.4 Phase 4: Explanation of the Anti-Phishing Software Philosophy Based on Bayes' Rule

The lecture of this phase started with probability and statistic theory. More specifically, it concluded the following: defining the probability and expressing it as a number (0-1), kinds of probabilities (classical - frequentist - subjectivist), prediction based on probabilities, conditional probability and Bayes' theorem.

We then presented an analysis of the phishing emails created by students who attended the same module the previous year (the previous year module stopped in phase 2). In total, there were 164 phishing emails crafted by previous year students on the same victim – target. The main subject analysis of these emails showed that they can be classified into six categories and combination of these. The six theme categories of the phishing emails, based on the victim's internet profile are: profession as a pilot, running activity, holidays, healthy diet, beer consumption, a friend called Josh.

Furthermore, we assumed that the hypothetical target recipient of these emails had received also 200 legitimate, non-phishing emails in the past month. The target provided feedback on the analysis of his non-phishing emails. More specifically, we knew the classification of these 200 non-phishing emails according to the six theme categories. The total data we had, are illustrated in table 1:

Table 1: The classification of the emails in the designated categories

Email's theme is about	Non phishing emails (200 in total)	Phishing emails (164 in total)
victim's profession	56	95
running activity	38	43
victim's profession and running	4	30
heathy diet	9	14
running and health diet	3	8
beers	15	23
holidays	47	3
friend Josh	4	48
friend Josh and victim's profession	1	26
friend Josh and beers	0	6

According to the data of the Table 1, we wanted to know the probability of an email to be phishing, given its theme is about the victim's profession. So, we are looking about P(Phishing|Profession). We can calculate this probability easily (according to the Bayes rule), as follows:

$$P(\text{Phishing}|\text{Profession}) = \frac{P(\text{Profession}|\text{Phishing}) \times P(\text{Phishing})}{P(\text{Profession})}$$

Using the data of Table 1, we calculate the following probabilities:

- P (Profession|Phishing)= 95/164 = 0,58
- P (Phishing)= 164/364 = 0,45
- P (Profession)= (95+56)/364 = 0,41
- So, P (Phishing|Profession) = 0,64

That means that when the hypothetical target of our scenario receives an email which its theme is about his profession, then 64 % it is a phishing email.

With the same way described in the previous paragraph, we calculated that P(Phishing|Running) = 0.55 and so on. As we applied Bayes' rule to each data point, the mathematical operations became increasingly complex. Especially, if we need to find the probability of an email being phishing if it has two, three or four themes simultaneously. For example, if we wanted to examine the probability P(phishing|holidays, Josh, beers). This highlighted the need to develop a Bayesian network that could directly provide the probability of an email being phishing based on specific indicators. By constructing this network, we could streamline the process, enabling it to automatically calculate the probability of phishing whenever relevant indicators were inserted.

To construct the Bayesian Network, first, we chose the nodes and found the connection among them. Then, we put probabilities in every node (Figure. 4).

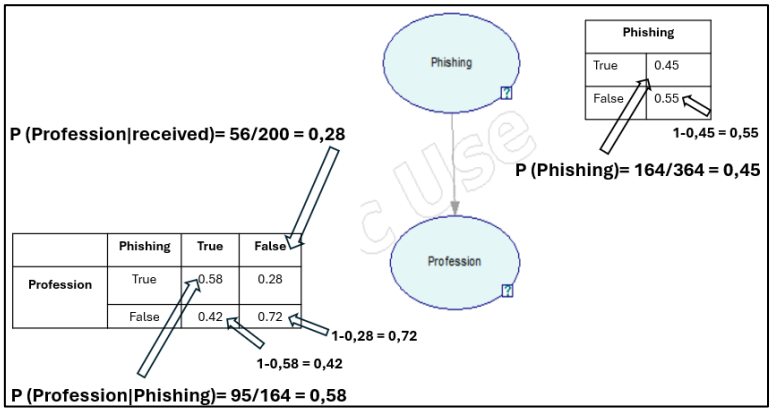

Figure 4: An example of the construction of our Bayesian network

The final version of the network, nodes and connections, is displayed in the Figure 5 (using GeNIe Academic software). In this Bayesian network, we put as evidences the themes an email is about (states: True – False), and we will receive as output the probability of this email to be phishing. For example, if an email theme is about healthy diet and running activity the probability of this email to be phishing is 68% (Figure 5).

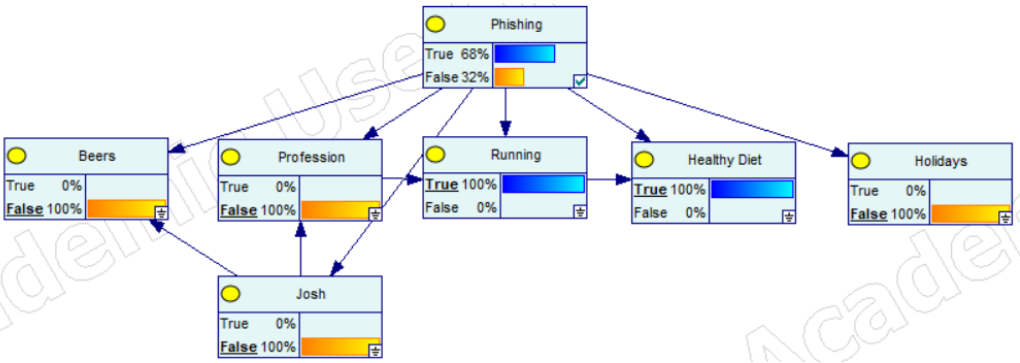

Figure 5: P(Phishing|Healthy_Diet,Running) = 0.68

This network was then implemented using Python programming language, programmed to recognize keywords within the text that correspond to the meaning of each node. The program was coded using nltk toolkit (Bird, 2006) for the email processing and pgmy (https://pgmpy.org) for constucting and estimating the Bayesian inference. For instance, if the words Christmas, visit, vacation, holiday, ticket, place, sightseeing were detected, that meant that the phishing email was included the theme of the node "holidays". When such keywords were detected, the network marked the respective node as true.

3.5 Phase 5: Practice on Bayes Rule and Bayesian Networks

In the last phase, we asked trainees to practice with Bayes rule and Bayesian networks. Participants calculated probabilities and drew their networks on a paper sheet we had given them (Figure. 6). They tried to construct a smaller Bayesian Network than the one described in phase 4.

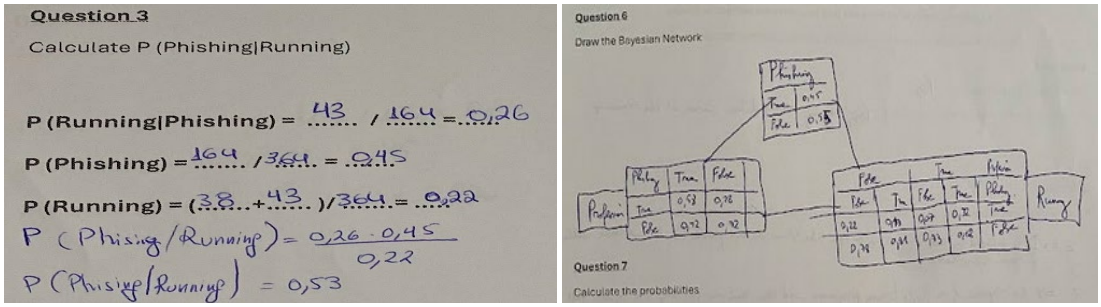

Figure 6: Examples of participants' practice exercises

4. Conclusions

Bayesian networks, a statistical method based on probabilities derived from prior data, is a valuable tool in cybersecurity for predicting outcomes in uncertain situations. Recognizing the importance of this method for cybersecurity trainees, we designed an innovative 360-degree educational approach to effectively teach it. Instead of following conventional teaching methods, we engaged trainees in an interactive and practical exercise. They were tasked with creating phishing emails for an imaginary person whose personality traits and behavior were deduced from his social media profile. This activity fostered an understanding of social engineering tactics.

Next, the trainees utilized a custom-built antiphishing software designed specifically for this course. The software, powered by a Bayesian network, analyzed the trainees' phishing emails and provided a percentage indicating the likelihood of the email being identified as phishing. The Bayesian network was constructed using data from the previous academic year's trainees, ensuring relevance and practical applicability. This percentage-based feedback served as a strong motivator, encouraging trainees to actively engage with the subsequent training on Bayesian networks as a phishing protection method. The hands-on approach deepened their understanding of how Bayesian principles can predict risks and informed their decision-making in cybersecurity contexts.

This innovative approach not only enhanced the trainees' technical skills but also fostered their analytical thinking and problem-solving abilities, preparing them to tackle real-world cybersecurity challenges effectively. The evaluation of the responses revealed that the majority of trainees successfully applied Bayes' rule. However, the most frequent error was in calculating prior probabilities based on the provided data. Additionally, challenges were noted in designing Bayesian networks, particularly in identifying causal relationships between variables. These highlights the need for more hands-on training in this area to strengthen their practical skills.

References

Bird, S. (2006) NLTK: the natural language toolkit. In Proceedings of the COLING/ACL 2006 Interactive Presentation Sessions (pp. 69-72).

Burden, P., and Byrd, D. (2010) Methods for Reflective Teaching: Meeting the Need of All Students (5th ed.). New York: Library of Congress.

Cooper, C. and Herskovits, E. (1992) A Bayesian Method for the Induction of Probabilistic Networks from Data. Machine Learning, vol. 9, no. 4, pp. 309–347.

Chen Y.F. (2017) Security risks of smart phone and preventive strategies. Information Security Research, 13, 158-160.

Clark, R. (2009) Accelerating expertise with scenario based learning. Learning Blueprint. Merrifield, VA: American Society for Teaching and Development.

Dunham, K. (2004) Phishing Isn't So Sophisticated: Scary! Information Systems Security, 13(2), 2–7.

Eberhardt, J. (2015) Bayesian Spam Detection. Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal: Vol. 2: Iss. 1, Article 2.

Errington, E. (2010) Preparing Graduates for the Professions Using Scenario-based Learning. Australia: Post Pressed.

García, P. Amandi, A. Schiaffino, S. and Campo, M. (2005) Using Bayesian Networks to Detect Students' Learning Styles in a Web-based education system. Proceedings of ASAI 2005, Argentine Symposium on Artificial Intelligence.

Godet, M. and Roubelat, F. (1996) Creating the future: the use and misuse of scenarios, Long Range Planning, Vol. 29, No. 2, pp.164-171.

Hart, S., Margheri, A., Paci F., Sassone, V. (2020) Riskio: A Serious Game for Cyber Security Awareness and Education, Computers & Security, Volume 95.

Jagatic, T. N., Johnson, N. A., Jakobsson, M. and Menczer, F. (2007) Social phishing. Communications of the ACM, 50(10), 94-100.

Jensen, F. (1996) An introduction to Bayesian Networks. Springer Verlag.

Khuda, I. (2021) Innovative Teaching Pedagogy for Teaching and Learning of Bayes' Theorem. Cankaya University Journal of Science and Engineering, 18(1), 61-71.

Khonji, M., Iraqi Y., and Jones, A. (2013) Phishing Detection: A Literature Survey. *in* IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091-2121.

Lappas, D. & Karampelas, P. (2023) Designing an Email Attack by Analysing the Victim's Profile. An Alternative Anti-Phishing Training Method. In n Proceedings of the 22nd European Conference on Cyber Warfare and Security, Athens, Greece, 22 - 23 June 2023.

Margetson, D., (1998) What counts as problem-based learning? Education for Health. 11:193-201.

Meyer T., Whateley B. (2004) Spam Bayes: Effective open-source, Bayesian based, email classification system. In CEAS.

Mokhtarian, E., Akbari, S., Jamshidi, F., Etesami, J., & Kiyavash, N. (2022) Learning Bayesian Networks in the Presence of Structural Side Information. Proceedings of the AAAI Conference on Artificial Intelligence, 36(7), 7814-7822.

Nadolski, R. J., Hummel, H. G. K., van den Brink, H. J., Slootmaker, A., Kurvers, H. J. and Storm, J. (2008). EMERGO: A methodology and toolkit for developing serious games in higher education. Simulation & Gaming: An Interdisciplinary Journal, 39(3), 338-352.

Raj, P., & Mittal, M. (2018) Detection of Phishing URLs using Bayes Net and Naïve Bayes and evaluating the risk assessment using Attributable Risk. International Journal of Computer Sciences and Engineering, *6*(5).

Seryasat, O.R. Ahmadi, S. Yousefi, P. Tat S. and Farzad Sanei, S. (2021) Recognizing phishing websites based on a Bayesian combiner.

Tandale, K.D., and Pawar, S.N. (2020) Different Types of Phishing Attacks and Detection Techniques: A Review. International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), 295-299.

Torten, R. Reaiche, C. Boyle, S. (2018) The impact of security Awareness on information technology professionals' behavior. Computers & Security. 79.

Vayansky, I., and Kumar, S. (2018) Phishing–challenges and solutions. Computer Fraud & Security, (1), 15-20.

Wang J., Neil, M., Fenton, N. (2020) A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model, Computers & Security, Volume 89, 2020, 101659, ISSN 0167-4048.

Wilkinson (1995) How to Build Scenarios. Wired Scenarios: 1.01, Special Edition, September, pp.74–81.

Williams, E., Beardmore, A., Joinson, A. (2017) Individual differences in susceptibility to online influence: A theoretical review, Computers in Human Behavior, Volume 72, Pages 412-421

Yang, X., Li, Y., Yang, Bo, Ying-fang, L. (2017) Phishing Website Detection Using C4.5 Decision Tree. DEStech Transactions on Computer Science and Engineering.

Zhang, H. Liu, G. Chow, T. Wenyin, L. (2011) Textual and Visual Content-Based Anti-Phishing: A Bayesian Approach. IEEE transactions on neural networks / a publication of the IEEE Neural Networks Council.