Submission received: 20th of September 2025
Revised: 16th of October 2025
Accepted: 25th of November 2025

EDUCATING AGAINST CYBERCRIME THROUGH BPMN-BASED PROCESSES

Anna Suchenia[1]

Abstract

Background and Objective: Cybercrime is rapidly expanding in both scale and sophistication, posing significant risks to users with limited technical knowledge, particularly older adults and individuals new to digital technologies. Traditional cybersecurity education often relies on technical explanations that may be difficult for these groups to understand. This paper aims to investigate whether Business Process Model and Notation (BPMN) can serve as an effective visual educational tool to enhance cybersecurity awareness by clearly illustrating how cyberattacks commonly unfold and where preventive actions can mitigate them.

Study Design/Materials and Methods: The study adopts a design-oriented, model-based research approach grounded in visual process representation. BPMN was applied to develop illustrative models of three prevalent online threats: phishing, smishing, and online shopping fraud. Each model represents the sequence of attacker and victim actions, key decision points, and critical moments where informed user behaviour can prevent or mitigate an attack. The models were designed to be adaptable for different age groups and levels of digital literacy. As the study is conceptual and focuses on model development rather than empirical validation, no statistical analysis was performed; therefore, confidence intervals and levels of statistical significance are not applicable.

Results: The resulting BPMN diagrams provide a structured and transparent visualisation of cyberattack progression, enabling clearer understanding of manipulation techniques and risk points. The models highlight actionable prevention steps and support comprehension of the human-factor vulnerabilities exploited in common cybercrime scenarios. BPMN proved suitable for representing cybersecurity threats in a way that is intuitive, process-oriented, and accessible to non-technical users.

Practical Implications: The proposed BPMN-based models can be directly applied in cybersecurity awareness programmes, educational workshops, and organisational training initiatives. They offer a standardised yet flexible framework for communicating cyber threats and preventive behaviours across diverse user groups. In practice, this approach may strengthen

[1] Cracow University of Technology, Poland, anna.suchenia@pk.edu.pl, ORCID: 0000-0003-4740-6027

DOI: 10.19253/reme.2026.01.006

user awareness, reduce susceptibility to social engineering attacks, and support the development of age-appropriate and inclusive cybersecurity education materials.

Conclusion and Summary: This study demonstrates the potential of BPMN as a visual and educational tool for improving cybersecurity awareness among users with varying levels of digital competence. By translating complex cyberattack mechanisms into clear, process-based diagrams, BPMN can bridge the gap between technical cybersecurity knowledge and everyday user understanding. While the findings are conceptual, they provide a foundation for future empirical research to evaluate the educational effectiveness of BPMN-based cybersecurity training in real-world contexts.

Keywords: Cybersecurity Education, BPMN, Visual Learning, Educational Technology

JEL classification: M15, L86, O33

Paper type: research study

1. Introduction

The rapid digitalisation of society, accelerated significantly by the COVID-19 pandemic, has resulted in a widespread shift towards online services such as e-government, telemedicine, and e-commerce (Suchenia, 2021). This digital transformation, while beneficial, has simultaneously increased user exposure to cyber threats. Cybercrime has become an increasingly frequent and damaging phenomenon, ranging from identity theft and phishing to more complex fraud schemes (Banasiński & Rojszczak, 2018). Vulnerable populations, such as older adults or individuals with low digital literacy, are often the most affected.

In response to these challenges, this paper proposes the use of Business Process Model and Notation (BPMN) as a visual educational tool to help illustrate how cybercrimes occur and what actions can be taken to prevent or respond to them. BPMN is widely used in business and IT contexts to model workflows and processes. We suggest that its intuitive visual style, when carefully adapted, can be applied to cybersecurity education in both formal and informal learning environments.

Rather than making definitive claims about BPMN's effectiveness for all user groups, we present this work as a conceptual and exploratory framework. The aim is to demonstrate how complex cyber threat scenarios can be modelled in BPMN to support awareness and understanding. These models may serve as the foundation for further research on cybersecurity education strategies tailored to different demographics.

Despite the significant increase in cybercrime and the growing number of vulnerable users, existing cybersecurity education tools often rely on textual or abstract explanations that are difficult to understand for non-technical audiences. Although various visualisation- and gamification-based methods have been proposed, there remains a lack of structured, standardised approaches capable of clearly representing the sequential logic of cyberattacks. While BPMN is widely used in business

and IT environments, its educational potential in cybersecurity awareness remains underexplored.

To address this gap, the present study examines how BPMN can be adapted for the visualisation of online fraud mechanisms and defensive actions. The goal is to determine whether BPMN can support a clearer understanding of threat progression, improve user awareness, and serve as a complementary tool in cybersecurity education.

This study is guided by the following research questions:

1. How can common cybercrime scenarios be modelled in BPMN so that they are understandable to users with limited digital skills?
2. What educational advantages does BPMN offer compared to traditional narrative descriptions of cyber threats?
3. How can BPMN-based visualisations support awareness-raising initiatives for older adults and other high-risk groups?

2. Literature Review

Cyberspace is broadly defined as a virtual environment enabling communication between digital devices via the Internet. Its global accessibility and low cost have encouraged governments, institutions and businesses to shift many operations online raising concerns over cybersecurity risks to individuals and critical infrastructure.

More than a technical domain, cyberspace also functions as a platform for social interaction. Research emphasises not only the fight against cybercrime, but also the importance of securing teleinformatics systems, especially those supporting essential services (Banasiński & Rojszczak, 2018). The anonymity of the Internet has made it a target for malicious actors ranging from cybercriminals to state sponsored groups engaging in espionage, data theft, and disinformation.

Defining cybersecurity remains complex. The NICCS describes it as the protection of information systems from unauthorised access, damage, or misuse, encompassing both technological and institutional measures such as law enforcement and diplomacy. According to Poland's Cybersecurity Act (July 5, 2018), it refers to the resilience of systems to threats affecting data confidentiality, integrity, availability and authenticity. The literature calls for a consistent taxonomy of cyber threats and stresses the importance of international cooperation and information sharing, especially given the global and decentralised nature of cyberattacks (Edgar & Manz, 2017).

2.1. BPMN

Business Process Model and Notation (BPMN), developed by OMG (2011), is a widely adopted standard for modelling business processes (Chinosi & Trombetta, 2012). It was designed to offer a universal, easily understandable notation for both technical and non-technical users. The BPMN 2.0 specification defines four types of diagrams: Process, Collaboration, Conversation and Choreography. BPMN includes

over 100 modelling elements, organised into three levels of detail (Silver, 2011), and grouped into four categories:
— Flow Objects (events, activities, gateways),
— Connecting Objects (sequence flows, message flows, associations),
— Swimlanes (pools, lanes),
— Artifacts (data objects, groups, text annotations).

Flow objects define key actions and events, gateways manage decision points, and connecting objects show control and communication flows. Numerous BPMN extensions have been developed to address more advanced modelling needs (Kluza et al., 2018), (Kluza et al., 2021), (Ligęza, 2011), (Lübke et al., 2008), (Weidlich et al., 2008), (Lindsay et al., 2003), (Mroczek & Ligęza, 2014), (Szpyrka et al., 2011), (Arevalo et al., 2016), (Trkman et al., 2016), (Yousfi et al., 2016), (Martinho et al., 2015), (Pillat et al., 2015) and (Kluza et al., 2016).

2.2. BPMN and Cybersecurity

Cybersecurity is increasingly critical as the scale and complexity of cybercrime continue to grow. Among the many approaches to strengthening protection, BPMN has emerged as a useful tool for modelling and understanding security processes. Research shows that identifying security requirements early in system design particularly through process modelling can significantly improve final system security. Several studies explore how BPMN can be applied to cybersecurity challenges. The study by Maines et al. (2017) proposes a theory-based framework for specifying cybersecurity requirements, compatible with BPMN and other modelling languages. Similarly, Meland & Gjære (2012) demonstrates how threats can be abstractly represented within basic BPMN process flows. The paper by Hacks et al. (2021) presents an innovative simulation method by mapping BPMN to the Meta Attack Language (MAL), applicable to SCADA, automotive and cloud environments. The study of Gaidels et al. (2018) compares BPMN extensions for modelling security requirements and maps them to an existing security taxonomy. Research by Zareen et al. (2020) provides case studies showing how BPMN supports organisational threat modelling. The paper of Maines et al. (2015) identifies limitations in BPMN's native support for cybersecurity and proposes an ontology to improve its expressiveness in this domain. In parallel, the literature stresses the importance of establishing a common taxonomy of cyber threats and motivations. Due to the global, decentralised nature of cybercrime, improving threat communication and coordination across international networks is essential for building more resilient security infrastructures.

2.3. Cybercrimes

Cybercrime has been steadily increasing, driven by rapid technological advancement and the widespread reliance on the Internet, particularly during the

COVID-19 pandemic. This growing threat highlights the urgent need for educational and social initiatives that promote safer online behaviour. BPMN models can play a valuable role in this context, offering visual representations of cybercrime processes and preventive actions that are accessible even to non-technical users. Thanks to their clarity and ability to simulate different paths, BPMN diagrams can support awareness campaigns by illustrating how specific scams unfold and how to respond effectively. Their use in training materials or public education can help demystify online threats and improve digital safety. Data from the Internet Crime Complaint Center (IC3), a U.S. government platform for reporting internet-related crime, reinforce the need for such educational efforts. In its Internet Crime Report 2020 (Federal Bureau of Investigation, Internet Crime Complaint Center, 2020), IC3 identified the most frequently reported cybercrimes (Fig. 1):

— Phishing/Vishing/Smishing/Pharming – deceptive attempts to obtain sensitive information;
— Non-Payment/Non-Delivery – transactions where products or payments never arrive;
— Extortion, Identity Theft, Spoofing, and Tech Support Scams – targeting both individuals and organisations;
— Business Email Compromise (BEC) and Romance Scams – manipulating trust for financial gain;
— Investment Fraud – promising false returns.

These data underscore the importance of broad cybersecurity education using accessible tools like BPMN to help users recognise and respond to these common threats.

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

Descriptors*		
Social Media	35,439	*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	35,229	

Figure 1. Most Frequently Reported Internet Crimes to IC3 in 2020

Source: Internet Crime Report, 2020.

Data from the report also show that younger age groups report fewer cybercrime incidents (Fig. 2), likely due to higher levels of digital literacy and familiarity with online security practices.

Victims		
Age Range[7]	Total Count	Total Loss
Under 20	23,186	$70,980,763
20 - 29	70,791	$197,402,240
30 - 39	88,364	$492,176,845
40 - 49	91,568	$717,161,726
50 - 59	85,967	$847,948,101
Over 60	105,301	$966,062,236

Figure 2. Cybercrime Victims by Age Group
Source: Internet Crime Report, 2020.

The data highlight the need for cybersecurity education across all age groups, with a particular focus on older adults, who are more frequently targeted by cybercrime. In contrast, younger users—likely due to greater digital exposure and awareness—tend to be less vulnerable. This trend reinforces the importance of tailored educational initiatives aimed at improving online safety among the most at-risk populations. Given the reported data, middle-aged and older adults appear to be the most vulnerable to cybercrime, often due to limited familiarity with digital tools and network operations. The growing reliance on the Internet—accelerated by the COVID-19 pandemic—has further exposed these groups to online threats. In this context, raising cybersecurity awareness through targeted educational and social initiatives is essential. BPMN models offer a practical tool to support these efforts. Their ability to visually represent cybercrime scenarios in a clear and structured way makes them suitable for both public education campaigns and formal learning environments. Animated or interactive diagrams can help illustrate how attacks unfold and what actions users should take to avoid becoming victims. By using BPMN in cybersecurity education, we can improve digital literacy across all age groups. These visualisations make complex threats more understandable and enable individuals to better recognise and respond to online risks, ultimately contributing to a safer digital society.

2.4. Cybercrimes in BPMN

This section presents common types of internet fraud in a clear and accessible way, using BPMN diagrams to visualise how these scams typically unfold. The examples aim to help users understand the mechanisms behind each fraud, recognise warning signs, and learn both preventive measures and recommended actions if victimised.

One such scam is smishing, a form of phishing that uses SMS or messaging apps instead of phone calls. In this case, the attacker sends a deceptive message urging the recipient to click a link, call a number, or reply via text often under the pretense of urgency or official communication (Fig. 3).

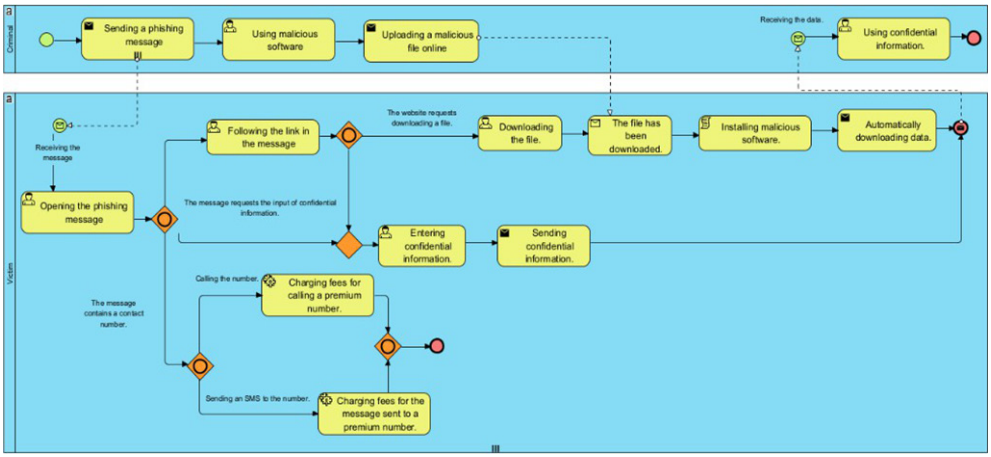

Figure 3. Smishing Process in BPMN

Source: author's own work.

In smishing attacks, the user receives a deceptive SMS or message via social platforms urging immediate action such as clicking a link, calling a number, or replying via text. The link often leads to a spoofed website designed to harvest confidential information or prompt a malware download. Alternatively, calling or texting a premium-rate number may result in unexpected charges. In some cases, responding also triggers additional smishing or vishing attempts.

Attackers commonly impersonate trusted brands to build credibility. A notable example involved a fake InPost delivery notification: the victim was prompted via SMS to pay a symbolic fee (1 PLN) to prevent cancellation. The included link led to a counterfeit banking login page (Jones, 2021). As with phishing, it is essential not to engage with suspicious links or contact numbers and to verify the legitimacy of any request (Met Networks, n.d.).

Using BPMN diagrams, such as in Figure 4, the message verification process can be visualised. Simulations based on these diagrams allow users to observe potential decision paths, helping them identify critical points where caution is needed. This visual, scenario-based approach is especially useful in awareness campaigns, as it clarifies both how attacks work and what steps users can take to stay safe.

Throughout this section, we illustrate not only how various attacks unfold, but also how users can respond and recover if targeted.

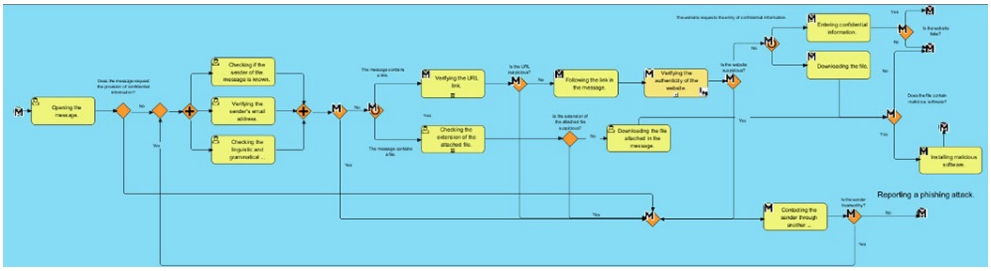

Figure 4. Message Verification Process in BPMN
Source: author's own work.

Another common cybercrime is Non-payment/Non-delivery fraud, which involves either failing to deliver goods after receiving payment or receiving goods without making a valid payment. In non-delivery scams, perpetrators list attractive offers on auction or shopping sites. Once the victim transfers funds, the scammer vanishes without sending the promised item (Fig. 5).

Some fraudsters operate through seemingly reputable platforms, persuading buyers to pay outside the system to avoid service fees. In more elaborate cases, entire fake e-commerce websites are created and promoted via social media or forums. These sites advertise unbeatable deals to lure victims. After collecting a large number of payments, the fraudulent site is taken down and often replaced by another (Internet Crime Complaint Center, 2021).

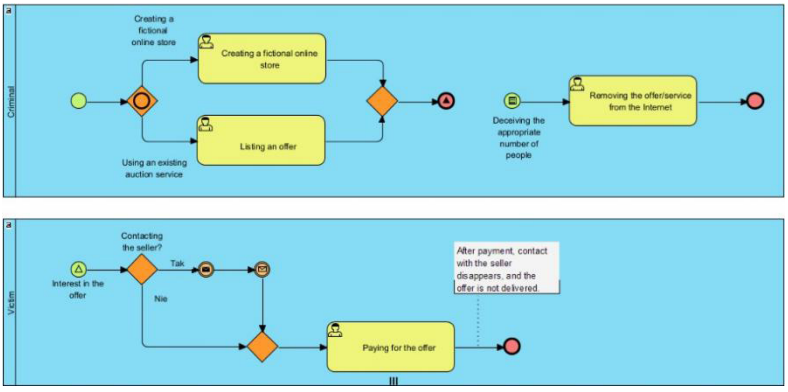

Figure 5. Non-delivery Fraud Process in BPMN
Source: author's own work.

To avoid falling victim to non-delivery scams, users should verify a website's authenticity and security, as outlined earlier. Payments should only be made through secure, platform-supported methods, never via external transfers. Agreeing to transactions outside the platform increases the risk of fraud. While cash on delivery may seem safer, it still does not guarantee the contents of the package before payment is

made. Figure 6 illustrates the recommended process for conducting secure online purchases (Internet Crime Complaint Center, 2021).

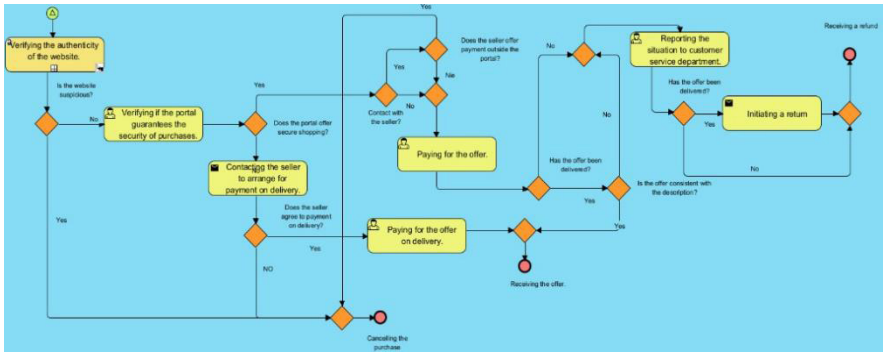

Figure 6. Secure Online Shopping Process in BPMN

Source: author's own work.

In non-payment fraud, the scammer aims to obtain goods or services without actually paying, unlike non-delivery fraud where the victim pays but receives nothing in return (Federal Bureau of Investigation, Internet Crime Complaint Center, 2020). The perpetrator typically sends a forged proof of payment to convince the seller that the transaction has been completed, prompting them to ship the goods or provide services (Fig. 7). Since many platforms only release funds after the buyer confirms receipt, sellers are often pressured to act quickly, sometimes without properly verifying payment. In some cases, scammers also impersonate auction or payment services by sending fake confirmation messages to further deceive the seller.

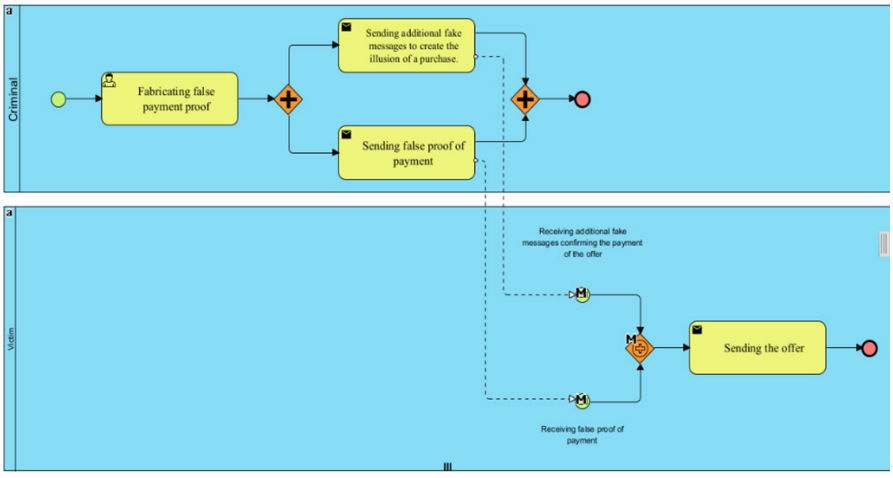

Figure 7. Non-payment Fraud Process in BPMN

Source: author's own work.

The most effective defense against non-payment fraud is verifying that payment has been received before fulfilling the order (Fig. 8). Sellers should never ship goods or provide services until the funds are confirmed in their account (Maimon et al., 2019).

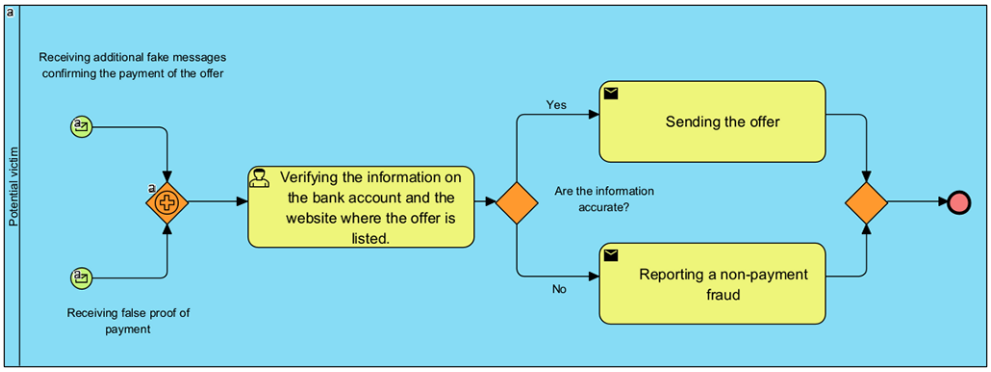

Figure 8. Verification of Purchase Information in BPMN
Source: author's own work.

The BPMN diagrams presented in this study were developed using a design-oriented methodology grounded in publicly available cybercrime reports, including the Internet Crime Complaint Center (IC3) datasets, law enforcement publications, and cybersecurity literature. The diagrams were constructed in accordance with BPMN 2.0 specifications, using a level of abstraction suitable for non-technical users while maintaining accurate process logic. The intention was not to replicate complete forensic scenarios but to capture essential steps of attacker-victim interaction in a pedagogically useful form. Although empirical validation has not yet been conducted, the models were reviewed for internal consistency, semantic correctness, and educational clarity. Future work will involve structured user testing to assess their effectiveness.

3. BPMN as an educational tool for cybersecurity awareness

Business Cybersecurity education requires methods that are both engaging and accessible, particularly for users with limited technical backgrounds. Business Process Model and Notation (BPMN) offers a way to visually represent the flow of cyberattacks and corresponding defense mechanisms. Its structured and standardised graphical syntax can help demystify complex concepts by showing how cybercrimes unfold step by step and what users can do in response. We propose BPMN as a tool to support scenario-based learning in cybersecurity education. This section outlines four ways BPMN can contribute to such efforts.

3.1. Visualising Threat Scenarios

A key strength of BPMN lies in its capacity to represent complex processes through clear, visual diagrams. In the context of cybersecurity, these diagrams can map out the sequence of actions involved in an attack, allowing users to follow how such incidents develop and what decisions or consequences arise at each stage. For instance, a phishing attempt can be visually modelled from the receipt of a fraudulent message to the point where sensitive data is compromised.

By presenting the process in a step-by-step visual format, BPMN helps demystify cyber threats, making them more accessible and easier to understand. This approach is especially beneficial for visual learners, as it supports better comprehension and retention through graphical representation.

3.2. Educational Use Cases by Audience

BPMN diagrams can be adapted to suit different age groups, helping ensure that cybersecurity education remains relevant, understandable and engaging for all learners. For younger audiences, simplified models can highlight fundamental safety habits such as avoiding password sharing or identifying suspicious links. For older adults, more comprehensive diagrams can walk through typical scam scenarios like phishing or smishing, showing how to assess the legitimacy of digital messages and requests.

These visual tools can be integrated into a variety of educational formats, including classroom lessons, community workshops, and online training sessions. By using BPMN in this way, educators can improve both comprehension and long-term retention, ultimately equipping individuals with the knowledge needed to navigate digital spaces more safely.

3.3. Visualising Protective Measures

Beyond outlining the structure of cyber threats, BPMN can also be used to illustrate practical steps for prevention and response. Diagrams can guide users through key security practices such as enabling two-factor authentication, identifying secure websites, or reporting suspicious messages and activity.

By visually mapping out these actions, BPMN helps simplify complex security procedures, making them more understandable and easier to follow, especially for individuals with limited technical experience. This approach turns abstract cybersecurity recommendations into concrete, visual instructions that users can apply with greater confidence.

3.4. Modelling applications security

In addition to supporting user education, BPMN can play a valuable role in the design and evaluation of secure software systems. Security analysts and developers

can use BPMN diagrams to represent the internal security mechanisms and protocols of an application, helping to identify weak points, potential vulnerabilities, and opportunities for enhancement. These models can act as visual blueprints during the software development lifecycle, ensuring that security considerations are addressed from the early design stages through to implementation.

The strength of BPMN lies in its flexibility: it can be used both to educate end-users about safe practices and to support professionals in building more secure systems. By combining these uses, BPMN offers a comprehensive framework for promoting cybersecurity awareness and resilience. Leveraging its visual clarity can help create a more informed public and a more secure digital environment across all levels of technical understanding.

3.5. Cybersecurity Education Approaches

Cybersecurity education includes a range of strategies such as awareness campaigns, simulation-based training, instructional videos, gamified learning environments, and hands-on workshops. Prior research emphasises that effective education must account for differences in digital literacy, cognitive load, and user experience, particularly among older adults and individuals with limited technological proficiency. Visualisation tools such as attack trees, threat maps, interactive simulations, or step-by-step scenarios have been shown to improve comprehension and retention by presenting threats in a more tangible and relatable form.

However, many of these tools lack standardisation, rely heavily on simplified or ad-hoc diagrams, or require significant prior knowledge. In contrast, BPMN provides a formalised, widely recognised notation designed to model complex workflows with precision and clarity. Despite this potential, its use in cybersecurity education is rarely explored, and empirical evidence on its pedagogical effectiveness remains limited. This study contributes to filling this gap by demonstrating how BPMN can visually represent cybercrime processes and facilitate an understanding of defensive behaviours.

4. Conclusions

This paper presents an exploratory investigation into the use of BPMN modelling as a means of depicting and explaining online cybercrimes within an educational context. Through several representative examples including smishing, phishing, and non-delivery scams, the study illustrates how BPMN diagrams can capture the underlying process logic of typical fraud schemes and visually communicate appropriate defensive actions. While the graphical expressiveness of BPMN suggests considerable potential for enhancing comprehension among non-technical users, its actual pedagogical effectiveness must be empirically evaluated.

It is important to emphasise that this work does not claim BPMN to be universally intuitive without prior instruction. Instead, here, the argument advanced is that BPMN provides a structured, formalised, and potentially scalable medium for communicating cyber risks, provided that its use is accompanied by appropriate teaching strategies, simplified visual support, and audience-specific guidance. Moreover, segmenting learners solely by age may be insufficient; factors such as socioeconomic background, prior digital experience, and cognitive load tolerance should also inform the design of cybersecurity education initiatives.

Future research will therefore focus on validating these BPMN-based models through classroom pilots, workshops, and online training programmes involving diverse user groups. Collaboration with educators and cybersecurity professionals is also planned to refine both the technical accuracy and the pedagogical usability of the diagrams.

From a practical standpoint, BPMN models can be readily incorporated into workshops, community training, and digital safety curricula. Recommended implementation strategies include:

— providing a simplified legend of BPMN symbols to support learners with limited technical backgrounds,
— employing colour coding or annotations to highlight threat indicators and recommended user actions,
— presenting scenarios sequentially to allow learners to follow the unfolding of an attack step by step,
— integrating BPMN diagrams with interactive tasks, such as identifying fraud cues or practising decision making,
— adjusting diagram complexity to the needs of different audiences, for example, using simplified flows for older adults and more detailed representations for advanced learners.

These measures can enhance comprehension, foster more proactive security behaviours, and strengthen long-term cybersecurity awareness.

Given the conceptual nature of this study, empirical validation remains essential for assessing the educational value of BPMN-based materials. Subsequent research will therefore include pilot workshops, controlled experiments, and user studies aimed at evaluating comprehension, risk recognition, and behavioural responses across heterogeneous user groups. The insights gained from these evaluations will inform further refinement of the models and help establish their effectiveness as pedagogical tools.

References

1. Arevalo, C., Escalona, M., Ramos, I., & Domínguez-Muñoz, M. (2016). A metamodel to integrate business processes time perspective in BPMN 2.0. Information and Software Technology, 77, 17–33. DOI: 10.1016/j.infsof.2016.05.004

2. Banasiński, C., & Rojszczak, M. (Eds.). (2018). Cyberbezpieczeństwo. Zarys wykładu. Wolters Kluwer.
3. Chinosi, M., & Trombetta, A. (2012). BPMN: An introduction to the standard. Computer Standards & Interfaces, 34(1), 124–134. DOI: 10.1016/j.csi.2011.06.002
4. Edgar, T.W., & Manz, D.O. (2017). Research methods for cyber security. Syngress (Elsevier).
5. Federal Bureau of Investigation, Internet Crime Complaint Center. (2020). Internet Crime Report 2020. Retrieved January 15, 2026, from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
6. Gaidels, E., Gaidukovs, A., & Matulevičius, R. (2018). A coarse-grained comparison of BPMN extensions for security requirements modelling. In BIR Workshops 2018 (pp. 170–181). CEUR-WS.org. https://ceur-ws.org/Vol-2218/paper17.pdf
7. Hacks, S., Lagerström, R., & Ritter, D. (2021). Towards automated attack simulations of BPMN-based processes. In 2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC) (pp. 182–191). IEEE. DOI: 10.1109/EDOC52215.2021.00029
8. Internet Crime Complaint Center. (2021). Internet Crime Report 2020. Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf
9. Jones, C. (2021). Phishing, vishing, SMiShing, whaling and pharming: How to stop social engineering attacks. Expert Insights. Retrieved January 15, 2026, from https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/
10. Kluza, K., Jobczyk, K., Wiśniewski, P., & Ligęza, A. (2016). Overview of time issues with temporal logics for business process models. Annals of Computer Science and Information Systems, 8, 1115–1123. DOI: 10.15439/2016F328
11. Kluza, K., Kagan, M., Wiśniewski, P., Adrian, W. T., Jemioło, P., Suchenia, A., & Ligęza, A. (2021). Using a semantic-based support system for merging knowledge from process participants. In M. L. Owoc & M. Pondel (Eds.), Artificial intelligence for knowledge management (AI4KM 2019) (pp. 1–16). Springer. DOI: 10.1007/978-3-030-85001-2_1
12. Kluza, K., Wiśniewski, P., Ligęza, A., Suchenia, A., & Wyrobek, J. (2018). Knowledge representation in model driven approach in terms of the Zachman framework. In L. Rutkowski, R. Scherer, R. Tadeusiewicz, L. A. Zadeh, & J. M. Zurada (Eds.), Artificial intelligence and soft computing (pp. 689–699). Springer. DOI: 10.1007/978-3-319-91262-2_60
13. Ligęza, A. (2011). A note on a logical model of an inference process: From ARD and RBS to BPMN. In M. Nycz (Ed.), Knowledge acquisition and management (Research Papers of Wrocław University of Economics, No. 232, pp. 41–49). Publishing House of Wrocław University of Economics.
14. Lindsay, A., Downs, D., & Lunn, K. (2003). Business processes—Attempts to find a definition. Information and Software Technology, 45(15), 1015–1019. DOI: 10.1016/S0950-5849(03)00129-0
15. Lübke, D., Schneider, K., & Weidlich, M. (2008). Visualizing use case sets as BPMN processes. In 2008 3rd International Workshop on Requirements Engineering Visualization (REV'08) (pp. 21–25). IEEE. DOI: 10.1109/REV.2008.8

16. Maimon, D., Santos, M., & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. Journal of Crime and Justice, 43(1), 39–58. DOI: 10.1080/0735648X.2019.1691857
17. Maines, C.L., Llewellyn-Jones, D., Tang, S., & Zhou, B. (2015). A cyber security ontology for BPMN-security extensions. In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (pp. 1350–1355). IEEE. DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.265
18. Maines, C.L., Zhou, B., Tang, S., & Shi, Q. (2017). Towards a framework for the extension and visualisation of cyber security requirements in modelling languages. In 2017 10th International Conference on Developments in eSystems Engineering (DeSE) (pp. 71–76). IEEE. DOI: 10.1109/DeSE.2017.29
19. Martinho, R., Domingos, D., & Varajão, J. (2015). CF4BPMN: A BPMN extension for controlled flexibility in business processes. Procedia Computer Science, 64, 1237–1244. DOI: 10.1016/j.procs.2015.08.509
20. Meland, P.H., & Gjære, E.A. (2012). Representing threats in BPMN 2.0. In 2012 International Conference on Availability, Reliability and Security (ARES) (pp. 101–108). IEEE. DOI: 10.1109/ARES.2012.13
21. Met Networks. (n.d.). What is phishing, vishing, SMiShing and pharming? Retrieved January 15, 2026, from http://met-networks.com/phishing-vishing-smishing-pharming/
22. Mroczek, A., & Ligęza, A. (2014). A note on BPMN analysis: Towards a taxonomy of selected potential anomalies. Annals of Computer Science and Information Systems, 2, 1097–1102. DOI: 10.15439/2014F185
23. Object Management Group. (2011). Business Process Model and Notation (BPMN), Version 2.0. https://www.omg.org/spec/BPMN/2.0/
24. Pillat, R.M., Oliveira, T.C., Alencar, P.S.C., & Cowan, D.D. (2015). BPMNt: A BPMN extension for specifying software process tailoring. Information and Software Technology, 57, 95–115. DOI: 10.1016/j.infsof.2014.09.004
25. Silver, B. (2011). BPMN method and style: With BPMN implementer's guide (2nd ed.). Cody-Cassidy Press.
26. Suchenia, A. (2021). Towards a taxonomy of business process and its anomalies. International Journal of Computer Science and Network Security, 21(11), 230–240. DOI: 10.22937/IJCSNS.2021.21.11.32
27. Szpyrka, M., Nalepa, G.J., Ligęza, A., & Kluza, K. (2011). Proposal of formal verification of selected BPMN models with Alvis modeling language. In F. M. T. Brazier, K. Nieuwenhuis, G. Pavlin, M. Warnier, & C. Badica (Eds.), Intelligent distributed computing V (Studies in Computational Intelligence, Vol. 382, pp. 249–255). Springer. DOI: 10.1007/978-3-642-24013-3_26
28. Trkman, M., Mendling, J., & Krisper, M. (2016). Using business process models to better understand the dependencies among user stories. Information and Software Technology, 71, 58–76. DOI: 10.1016/j.infsof.2015.10.006
29. Weidlich, M., Decker, G., Großkopf, A., & Weske, M. (2008). BPEL to BPMN: The myth of a straight-forward mapping. In R. Meersman, Z. Tari, & P. Herrero (Eds.), On the move to meaningful internet systems: OTM 2008 (Lecture Notes in Computer Science, pp. 265–282). Springer. DOI: 10.1007/978-3-540-88871-0_19

30. Yousfi, A., Bauer, C., Saidi, R., & Dey, A.K. (2016). uBPMN: A BPMN extension for modeling ubiquitous business processes. Information and Software Technology, 74, 55–68. DOI: 10.1016/j.infsof.2016.02.002
31. Zareen, S., Akram, A., & Ahmad, S.K. (2020). Security requirements engineering framework with BPMN 2.0.2 extension model for development of information systems. Applied Sciences, 10(14), 4981. DOI: 10.3390/app10144981