

Toward a phishing attack ontology

Ítalo Oliveira^{1,2,*}, Rodrigo F. Calhau^{2,3} and Giancarlo Guizzardi²

¹*Conceptual and Cognitive Modeling Research Group (CORE), Free University of Bozen-Bolzano, Bolzano, Italy*

²*Semantics, Cybersecurity & Services Group, University of Twente, Enschede, Netherlands*

³*Ontology & Conceptual Modeling Research Group (NEMO), Federal University of Espírito Santo, Vitória, Brazil*

Abstract

Phishing attacks are the most common form of social engineering where attackers intend to deceive targeted people into revealing sensitive information or installing malware. To understand the dynamics of phishing attacks and design suitable countermeasures, particularly the promotion of phishing awareness, cybersecurity researchers have proposed several domain conceptual models and lightweight ontologies. Despite the growing literature in ontology engineering highlighting the advantages of employing upper and reference ontologies for domain modeling, current phishing attack models lack ontological foundations. As a result, they suffer from a number of shortcomings, such as false agreements, informality, and limited interoperability. To address this gap, we propose a *Phishing Attack Ontology* (PHATO) grounded in the *Reference Ontology for Security Engineering* (ROSE) and the *Common Ontology of Value and Risk* (COVER), which are both founded in the *Unified Foundational Ontology* (UFO). Our proposal is represented through the OntoUML ontology-driven conceptual modeling language, benefiting from its ecosystem of tools and domain ontologies. We also discuss some implications of PHATO for the design of anti-phishing countermeasures.

Keywords

phishing attack, social engineering, cybersecurity, phishing attack ontology, reference ontology for security engineering, common ontology of value and risk, unified foundational ontology

1. Introduction

In cybersecurity, social engineering is a type of attack in which the attacker exploits human vulnerabilities to breach security goals (confidentiality, integrity, availability, etc.) [1]. Phishing attacks are the most common form of social engineering where attackers intend to deceive targeted people into revealing sensitive information or installing malware [2]. In 2022, the Internet Crime Complaint Center of FBI (Federal Bureau of Investigation) reported more incidents of phishing than any other type of computer crime in the U.S. [2]. The same report defines phishing as “The use of unsolicited email, text messages, and telephone calls purportedly from

ER2023: Companion Proceedings of the 42nd International Conference on Conceptual Modeling: ER Forum, 7th SCME, Project Exhibitions, Posters and Demos, and Doctoral Consortium, November 06-09, 2023, Lisbon, Portugal


*Corresponding author.

✉ i.j.dasilvaoliveira@utwente.nl (Í. Oliveira); calhau@ifes.edu.br (R. F. Calhau); g.guizzardi@utwente.nl (G. Guizzardi)

🌐 <https://people.utwente.nl/i.j.dasilvaoliveira> (Í. Oliveira); <https://people.utwente.nl/r.calhau> (R. F. Calhau); <https://people.utwente.nl/g.guizzardi> (G. Guizzardi)

🆔 0000-0002-2384-3081 (Í. Oliveira); 0009-0006-6051-2165 (R. F. Calhau); 0000-0002-3452-553X (G. Guizzardi)

© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

a legitimate company requesting personal, financial, and/or login credentials”[2]. It is clear that phishing attacks involve different ways of combining technical and social elements.

Because of that, to understand the dynamics of phishing attacks and design appropriate countermeasures, such as phishing awareness training, cybersecurity researchers have proposed several domain conceptual models, lightweight ontologies, and informal conceptualizations of phishing [3, 4, 5, 6, 7, 8, 9, 10]. Despite the growing literature in ontology engineering highlighting the advantages of employing upper and reference ontologies for domain modeling, all current phishing attack models lack explicit ontological foundations.

A foundational (top-level or upper) ontology is a specific consistent set of ontological theories, capable of providing support to the tasks of domain analysis, conceptual clarification, and meaning negotiation — that are critical when one has to build an ontology as a computational artifact [11]. There is evidence that top-level ontologies help with the development of high-quality core and domain ontologies, improving their consistency and interoperability [12]. A (well-founded) core ontology specifies, under a foundational ontology, the central concepts and relations of a given domain (e.g., Risk, Value, Trust, Security, etc.). Upper ontologies effectively contribute to detecting and preventing ontology design mistakes [13], enhancing the quality and interoperability of domain and core ontologies [14]. The following analogy helps to clarify this point: foundational ontologies and reference domain ontologies work as *ontology engineering frameworks*, by accelerating and improving the practice of ontology engineering, just like web development frameworks (e.g., React, Angular, Django, etc.) accelerate and improve the practice of web development.

As a result of that lack of explicit foundations, existing phishing ontologies may suffer from a number of known shortcomings, such as false agreements, informality, limited interoperability, and unintended instances. At minimum, the guidance provided by a foundational ontology can improve domain ontologies in these respects as shown, for instance, by [15] in relation to a popular cybersecurity ontology written in OWL. To address this gap, we propose a *Phishing Attack Ontology* (PHATO)¹, a well-founded phishing model, grounded in the *Reference Ontology for Security Engineering* (ROSE) [16] and the *Common Ontology of Value and Risk* (COVER) [17], which are both founded in the *Unified Foundational Ontology* (UFO) [18]. Our proposal is represented through the OntoUML ontology-driven conceptual modeling language, benefiting from its ecosystem of tools and domain ontologies. We also discuss some implications of PHATO for the design of anti-phishing countermeasures.

The remainder of this paper is structured as follows: Section 2 presents several common elements about phishing attacks that will be helpful to support our proposal. Section 3 presents our ontological foundations with regard to the domains of value, risk, and security. Section 4 presents the main contributions: a *Phishing Attack Ontology* (PHATO). The same Section 4 briefly discusses some implications for the design of anti-phishing countermeasures. Section 5 debates related work. Section 6 finishes with limitations and future work.

¹The acronym plays with two related ideas: in Portuguese, “phato” - when the ‘ph’ is pronounced like an ‘f’ - sounds like “fato” (*fact*, in English); when it is pronounced or like a ‘p’, it sounds like “pato” (*duck*), which is a Brazilian slang for gullible. Both senses come together in the idea that phishing involves lying about facts to deceive a target.

2. Elements of phishing attacks in cybersecurity

Phishing is a form of social engineering attack, along with baiting, pretexting, tailgating, ransomware, impersonation on the help desk, diversion theft, dumpster diving, shoulder surfing, *Quid Pro Quo*, pop-up windows, robocalls, reserve social engineering, online social engineering, phone social engineering, stealing important documents, fake software, pharming, SMSishing, whitelisting flow [19], and potentially others.

The word “phishing” is a variation of the term “fishing” where the act of phishing resembles that of fishing in the following sense: the attacker lures a victim by using a sort of bait, then fishes for personal or confidential information from the victim [20]. Jakobsson [21] describes it as the “marriage of technology and social engineering”, remarking that successful attacks use both of these components in a strategic manner. Because of that, to prevent phishing attempts and their consequences, one should understand both elements.

There are many definitions of phishing in the literature (for a list with 113 distinct definitions, see [10]). According to this study, phishing can be defined as a “scalable act of deception whereby impersonation is used to obtain information from a target” [10]. The attacker can utilize various channels (emails, instant messages, voice calls, etc.) to either deceive the victim directly by a scam or to deliver payload through an indirect manner with the goal of obtaining personal or confidential information (login, passwords, bank account number, etc.) from the victim [20]. Sometimes, phishing involves tricking people into making them install malware, such as ransomware, which, then, will enable the stealing of confidential information or other asset. The damage caused by successful phishing attacks includes not only financial loss but also loss of reputation, fines from regulations, reduced productivity, intellectual property theft, and national security risk, affecting individuals, companies, and states.

Because phishing attacks cleverly exploit *human vulnerabilities*, they can circumvent the vast majority of an organization’s or individual’s security measures. As put by [22], it doesn’t matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish. Wangs [23, 5] enumerates (non-exhaustively) many vulnerabilities according to the following classification:

- **Cognition and Knowledge:** Ignorance, inexperience, thinking set and stereotyping, prejudice or bias, conformity, intuitive judgment, low level of need for cognition, heuristics, and mental shortcuts.
- **Behavior and Habit:** Laziness, carelessness and thoughtlessness, fixed-action patterns, habitual behaviors.
- **Emotions and Feelings:** Fear, curiosity, anger, excitement, tension, happiness, sadness, disgust, surprise, guilt, impulsion, fluke mind.
- **Human nature:** Self-love, sympathy, helpfulness, greed, gluttony, lust.
- **Personality traits:** Conscientiousness, extraversion, agreeableness, openness, neuroticism.
- **Individual characters:** Credulity, friendliness, kindness and charity, courtesy, humility, diffidence, apathy, hubris, envy.

According to [24], the most common form of phishing attacks includes three key components: the *lure*, the *hook*, and the *catch*. The lure consists of a phisher spamming a large number of

users with an email message that appears to be from some legitimate institution that has a presence on the Internet. The message often uses a convincing story to encourage the user to follow a URL hyperlink embedded in the email to a website controlled by the phisher and to provide it with certain requested information. The social engineering aspect of phishing attacks typically makes itself known in the lure, as the spam offers some plausible reason for the user to provide confidential information to the website that is hyperlinked by the spam. The hook commonly consists of a website that imitates the appearance of a reputable agent (say, a famous company's website). The goal of the hook is for victims to be directed to it via the lure portion of the attack and for the victims to disclose confidential information to the site. The catch involves the phisher making use of the collected information for some illegal purpose such as fraud or identity theft.

Phishing attacks can be classified in different ways (see, for instance, [9]). Frequently, the literature mentions "spear phishing" when the decoy is personalized to trick a specific individual or organization; "whaling phishing" when the attacker targets specifically senior executives or high-profile individuals; "vishing phishing" occurs if the attacks are performed via voice over the internet protocol (VoIP); "interactive voice response phishing" is performed by using an interactive voice response system to make the target enter the private information as if it is from a legitimate business or bank. "Business Email Compromise Phishing" mimics the whaling by targeting big "fishes" in corporate businesses in order to get access to their business emails, calendars, payments, accounting, or other private information. [19]

3. Background: value, risk, and security

The *Unified Foundational Ontology* (UFO) is a domain-independent axiomatic theory developed to contribute to the foundations of Conceptual Modeling [25, 18]. It is one of the most used foundational ontologies in conceptual modeling [26], and it has been successfully employed in many projects in different countries, by academic, government, and industrial institutions in the development of core and domain ontologies in different domains (e.g., Trust, legal relations and Constitutional Law, Risk and Value, Service, Software Requirements and Anomalies, Discrete Event Simulation, etc.) [25]. For our purposes, it suffices to say ontological distinctions of UFO are built-in OntoUML general-purpose modeling language. This means that OntoUML models are created by the iterative instantiation of ontology design patterns, each of which represents a UFO micro-theory.

Taking into consideration risk treatment options defined by ISO 31000, the *Reference Ontology for Security Engineering* (ROSE) [16] describes the general entities and relations of the security engineering domain, making use of an adapted version of the *Common Ontology of Value and Risk* (COVER) to capture the value and risk-related notions². ROSE understands the domain of security as the *intersection* between the domain of value and risk, understood under the terms of the COVER [17], and the dispositional theory of prevention presented in [27]. The latter extends UFO to explain how certain types of events are prevented or interrupted due to the occurrence of other events of specific types. From this perspective, an SECURITY MECHANISM is an OBJECT (of any kind) purposely designed to create value by preventing RISK EVENTS.

²Files related to ROSE can be found in the following public repository: <https://purl.org/security-ontology>.

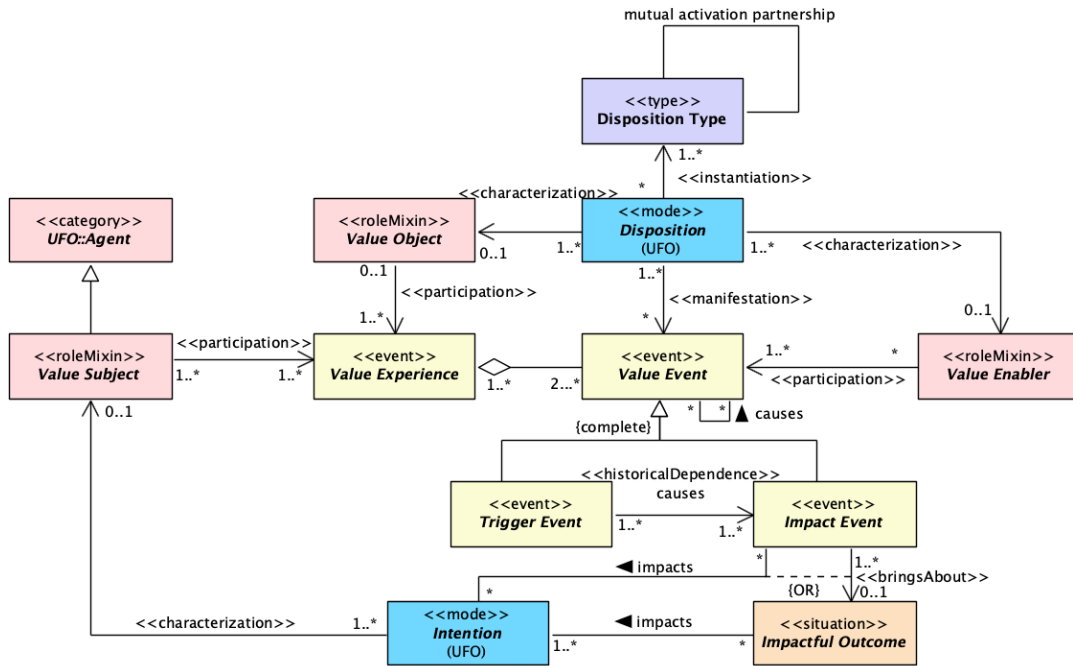


Figure 1: Value Experience, adapted from [17, 16].

In COVER³, whose fragment is depicted in Figure 1, value is a relational mode that emerges from the relations between the capacities (DISPOSITIONS) of certain objects and the INTENTIONS of an AGENT. The manifestations of these capacities are EVENTS that *bring about* a SITUATION that *impacts* or satisfies the INTENTION of a given AGENT (a VALUE SUBJECT)—in UFC-C, a goal is understood as the propositional content of an INTENTION [28], which is an internal commitment that inheres in an AGENT, which specializes OBJECT. Risk is the anti-value: RISK EVENTS are the manifestations of certain DISPOSITIONS (namely, THREAT CAPABILITIES and VULNERABILITIES), and, sometimes, INTENTIONS that inhere in an AGENT; these EVENTS *bring about* a SITUATION that *hurts* the INTENTION of a given AGENT (a RISK SUBJECT), as shown by Figure 2. Analogous to value, security (Figure 3) is also a relational mode that emerges from the relations between the (control) capabilities of OBJECTS and the INTENTIONS of an AGENT, particularly a PROTECTED SUBJECT; however, manifestations of these capabilities *bring about* a SITUATION that *impacts* the INTENTION of an AGENT in a very specific way: *preventing* RISK EVENTS [16].

Using the prevention theory described in [27], ROSE understands that THREAT CAPABILITY, VULNERABILITY, and, sometimes, INTENTION are dispositions associated with types whose instances maintain a *mutual activation partnership* to each other⁴. This means that a THREAT

³The OntoUML stereotype connects types and relations in these models to ontological categories of monadic and relational universals in UFO, respectively. For their ontological justification and semantics, one should refer to [18]. Moreover, the colors in these diagrams represent a color convention used by the OntoUML community: object types are represented in pink, intrinsic aspect types in blue, situation types in orange, event types in yellow, and higher-order types in darker blue.

⁴For simplicity, the diagram of Figure 2 omits the mutual activation partnership relations between THREAT CAPABILITY

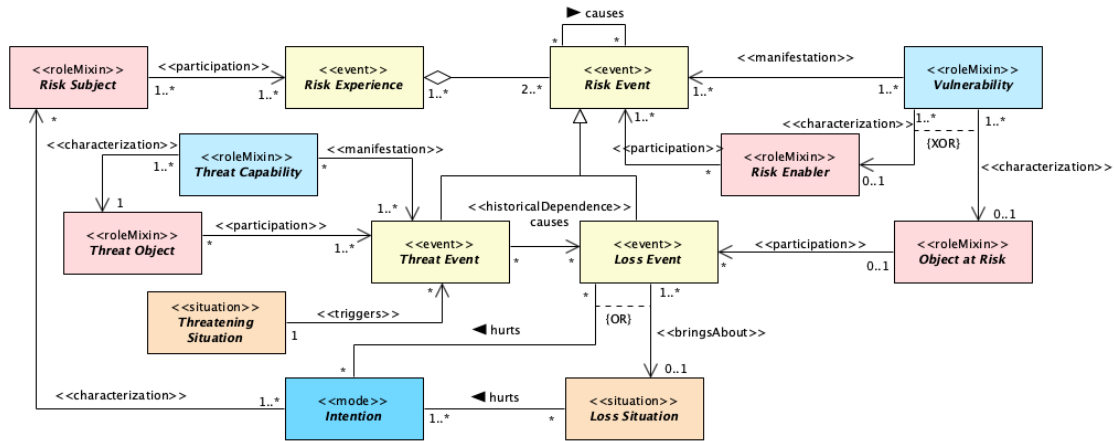


Figure 2: Risk Experience, adapted from [17, 16].

OBJECT can only manifest its THREAT CAPABILITY if a VULNERABILITY can be exploited; if the THREAT OBJECT participates in an ATTACK (an ACTION, an intentional EVENT), then the INTENTION is also required. Analogously, a VULNERABILITY is only manifested in the presence of a THREAT CAPABILITY. From a security point of view, the importance of this *generic dependence* relation among these entities is that it determines multiple ways by which security measures can work: the removal of any of them from the situation that could activate them all together implies the prevention of the associated RISK EVENT. In general, mutual activation partners compose the conditions of activation of any DISPOSITION, as shown by Figure 1. This relation generalizes the role of enabler objects (VALUE ENABLER, RISK ENABLER, THREAT ENABLER, and so on), which aggregate ancillary DISPOSITIONS with regard to THREAT CAPABILITY, VULNERABILITY, etc.

A SECURITY MECHANISM is always designed by an AGENT called the SECURITY DESIGNER to be a *countermeasure* to events of a particular type (RISK EVENT TYPE) [27, 16]. When an OBJECT is made to be a countermeasure to certain types of events, it aggregates capabilities whose manifestations ultimately prevent these EVENT TYPES in a systematic fashion. The AGENT creating a SECURITY MECHANISM is not necessarily the one protected by its proper functioning, i.e., the PROTECTED SUBJECT. However, both agents have INTENTIONS that are positively impacted by this proper functioning. For example, the government designs policies for public safety, and the functioning of such policies satisfies some goals the government had when designing them but also satisfies the goal of people who want to be safe. Sometimes, the PROTECTED SUBJECT is the same AGENT as the SECURITY DESIGNER, such as when a person places an electric fence surrounding their own house.

As shown in Figure 3, a SECURITY MECHANISM is an OBJECT, which may be a simple physical object like a wall, a high-tech air defense system, an AGENT like a policeman, a social entity like a security standard or anti-COVID-19 rules, that bears capabilities called CONTROL CAPABILITIES. The manifestation of this kind of capability is a CONTROL EVENT, which may come in the form of a chain of events that ultimately causes the CONTROL EVENT. The CONTROL EVENT is of a

TYPE, VULNERABILITY TYPE, and INTENTION TYPE but Figure 1 clearly states that types of dispositions hold that relationship with each other.

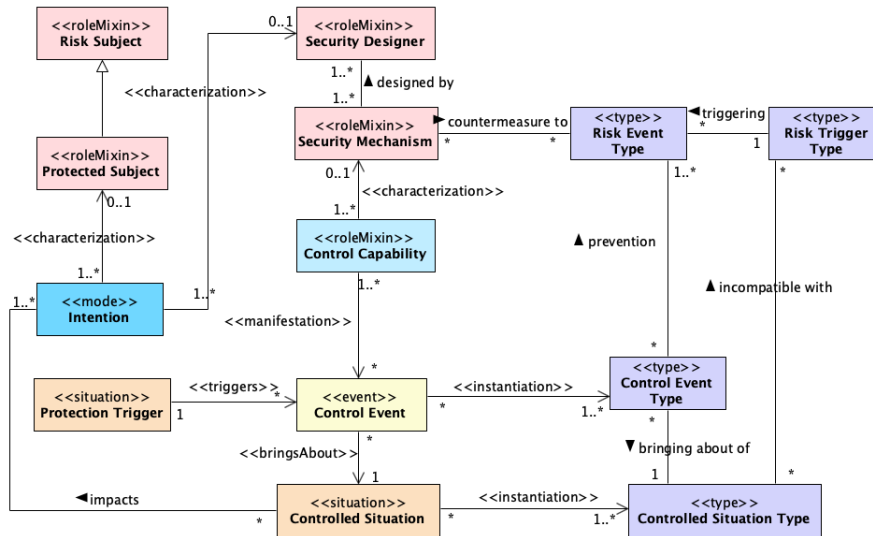


Figure 3: Security Mechanism, adapted from [16].

type (CONTROL EVENT TYPE) that prevents, directly or indirectly, events of a certain type (RISK EVENT TYPE). This is so because the CONTROL EVENTS bring about a CONTROLLED SITUATION, which is of a type that is *incompatible with* the types of SITUATIONS (RISK TRIGGER TYPE) that trigger RISK EVENTS of certain types.

Notice that CONTROL CAPABILITIES may characterize not only a SECURITY MECHANISM but also other objects. This means that a CONTROL EVENT can be, for instance, a single action that prevents certain types of RISK EVENTS, although not in a systematic fashion. For instance, when someone puts herself away from dangerous machines in a factory, she is manifesting her CONTROL CAPABILITIES by avoiding the danger and, therefore, generating value for herself, even though she is not a SECURITY MECHANISM. This is important to draw a distinction between a SECURITY MECHANISM whose actions are systematic and a CONTROL EVENT that may be the manifestation of a CONTROL CAPABILITY that does not inhere in a SECURITY MECHANISM.

4. A phishing attack ontology (PHATO)

Given the elements of phishing attacks described in Section 2 and our ontological foundations of Section 3, we propose a *Phishing Attack Ontology* (PHATO)⁵ by specializing the concepts of ROSE. Following this principle, we say a SCAMMER specializes an ATTACKER (a specialization of THREAT OBJECT) and *impersonates* an IMPERSONATED REPUTABLE AGENT (a person, a company, an organization, etc.). A SCAMMER has an INTENTION TO PHISH and the capability to do so, an IMPERSONATION CAPABILITY TO DECEIVE TARGET, which specializes THREAT CAPABILITY. It is clear that both intrinsic aspects are necessary for the manifestation of an event called IMPERSONATION OF REPUTABLE AGENT TO DECEIVE TARGET wherein a LURE participates (a given

⁵All related files of PHATO can be found at: <https://github.com/utwente-scs/phishing-ontology>

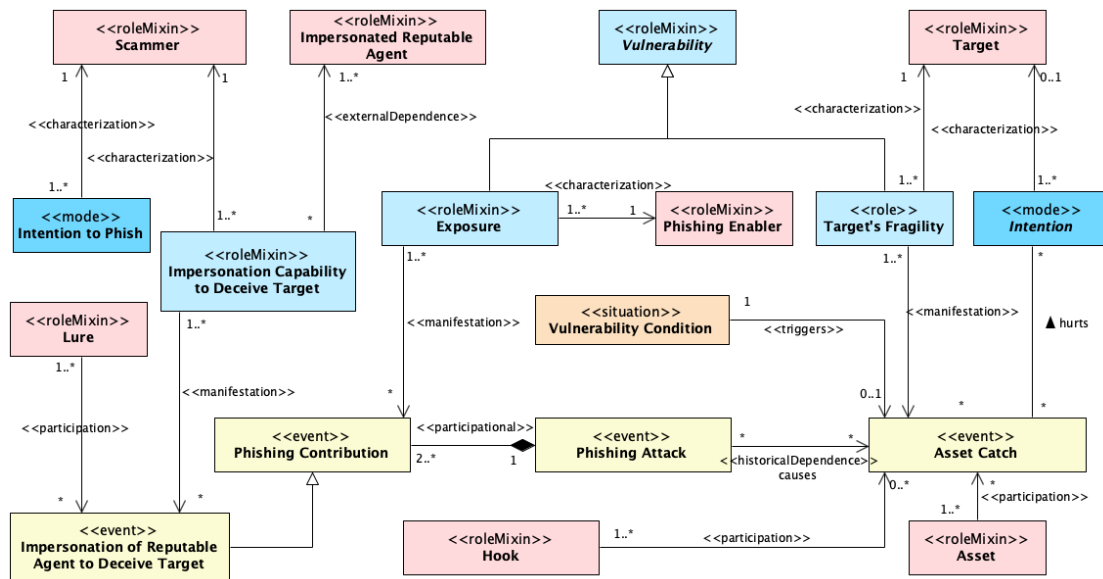


Figure 4: A Phishing Attack Ontology (PHATO).

email or SMS message, for example). Moreover, a third element must be in a SITUATION that can trigger a PHISHING CONTRIBUTION: an EXPOSURE of an ancillary entity called PHISHING ENABLER (for instance, the target’s phone number, email address, or computer network). In other words, there is a *mutual activation partnership* relation among INTENTION TO PHISH, IMPERSONATION CAPABILITY TO DECEIVE TARGET, and EXPOSURE. They are ultimately manifested by a complex event: a PHISHING ATTACK, a specialization of a THREAT EVENT.

At this point, human vulnerabilities usually do not play a major role yet. However, they are essential for the manifestation of an ASSET CATCH, an event wherein a HOOK and, naturally, an ASSET participate. A number of TARGET’S FRAGILITIES may be present in a VULNERABILITY CONDITION that triggers ASSET CATCHES, i.e., anyone can fall for a phish under the right conditions. ASSET CATCHES are LOSS EVENTS that *hurt* TARGET’S INTENTIONS to preserve her ASSETS (VALUE OBJECTS, OBJECT AT RISK). A TARGET is clearly a RISK SUBJECT.

As described in Section 2, there are many human mental attitudes that can play the role of a TARGET’S FRAGILITIES, such as INNOCENCE, FEAR, COMPLACENCY, DESIRE TO PLEASE, GREED, IGNORANCE, CURIOSITY, URGENCY, DISTRACTION, LONELINESS, just to cite a few. Figure 5 displays a non-exhaustive list of them, whereas Figure 4 presents the core elements of PHATO. Our ontology is rich enough to allow the specialization of several important concepts to achieve a better classification of the entities within the domain. For example, types of LURE can correspond to different strategies or messages employed by a SCAMMER. PHISHING ATTACK can be classified into SPEAR PHISHING ATTACK, WHALING PHISHING ATTACK, etc. The role of ASSET can be played by PASSWORD, LOGIN, etc. Instances of HOOK can be phishing websites. The rich scheme of PHATO may support the design of datasets or their integration for, e.g., machine learning tasks in this area.

With the support of ROSE and COVER, it is possible to assign a given likelihood that instances

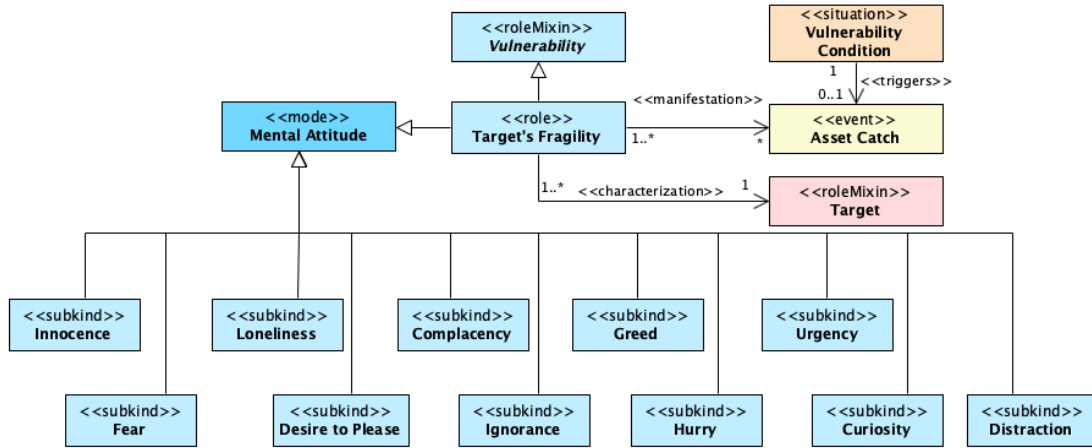


Figure 5: A non-exhaustive list of Target's Fragilities.

of a type of VULNERABILITY CONDITION trigger ASSET CATCH events of a particular type. We can say, for instance, that the more fragilities a person bears, the higher the chances of their falling for a phishing attack. Phishing awareness training, from this perspective, is a sort of CONTROL EVENT that eliminates or attenuates certain MENTAL ATTITUDES or builds new CONTROL CAPABILITIES so that these MENTAL ATTITUDES no longer play the role a fragility (e.g., when one is able to control their curiosity, greed or fear). This, in turn, helps preventing ASSET CATCHES to some degree. For example, the TARGET acquires cybersecurity knowledge through the training, which can eliminate TARGET'S IGNORANCE in relation to some common LURE. Consequently, the associated ASSET CATCH events are prevented because the type of SITUATION that could trigger them has been ruled out. Similarly, it is possible to assign a given likelihood for instances of a type of PHISHING ATTACK cause ASSET CATCH events of a specific type. In other words, we can analyze which kinds of PHISHING ATTACKS are the most successful at capturing ASSETS.

By representing a number of interconnected entities that are relevant for PHISHING ATTACKS and ASSET CATCH events, PHATO can support the design of suitable countermeasures. For example, phishing awareness training is one of the most efficient ways of preventing people from falling for a phish [29]. Figure 6 displays such a case where a PHISHING AWARENESS PROGRAM is designed to be a *countermeasure* to ASSET CATCH events of a certain type by the manifestation of PHISHING AWARENESS TRAINING wherein the TARGETS participate. In this case, a PHISHING AWARENESS PROGRAM is a social entity whose capabilities are manifested by PHISHING AWARENESS TRAINING, which may remove some of TARGET'S FRAGILITIES, therefore preventing certain types of ASSET CATCH event.

5. Related work

Although there are numerous ontology-based works in security and cybersecurity, recent literature reviews [30, 31, 32] have shown they are mostly focused on specific applications and

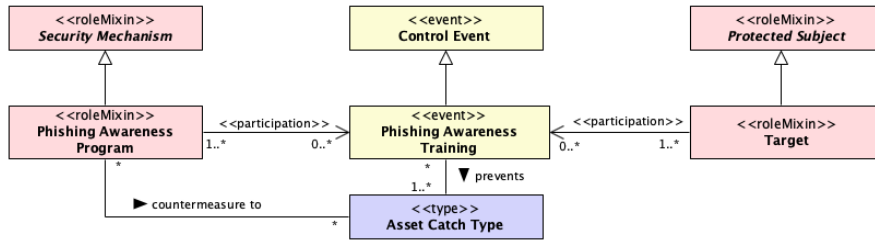


Figure 6: An example of anti-phishing countermeasure, Phishing Awareness Program.

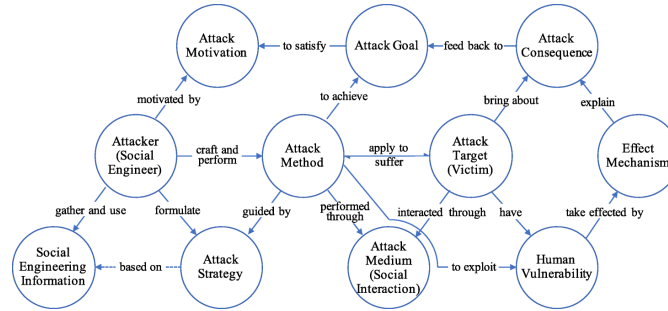


Figure 7: The domain ontology of social engineering in cybersecurity proposed by Wang *et al* [5].

lack ontological foundations. As a consequence, an in-depth ontological analysis of phishing attacks is missing. For example, in [3] the authors are interested in automated phishing detection with the aid of a proposed taxonomy. Similarly, in [6] a description logic and OWL ontologies are proposed to represent scenarios of e-mail phishing attacks. The latter also presents a list of ontology-based works, which are lightweight (DL, RDF, OWL, frames) and application-focused. A few of these works resemble an ontological account but they focus on social engineering in general, not phishing attacks. Even these offer no more than an OWL [4, 5] or UML-like [7, 8] ontology. Just like noticed by [30] for security ontologies, we could not find publicly any artifacts reported by this literature, which makes any evaluation more difficult (for instance, to check logical consistency and unintended instances). Therefore, to the best of our knowledge, the present work is the first analysis and conceptualization of phishing attacks employing a foundational ontology. For comparison, Figure 7 depicts an interesting proposal of a domain ontology of social engineering by Wang *et al* [5], where we can clearly notice the lack of ontological distinctions among the classes (objects, events, modes, situations, etc.). This may yield too many unintended instances, as shown by Oliveira *et al* [15] by analyzing a well-known cybersecurity ontology.

6. Final considerations

Dealing appropriately with phishing attacks is currently one of the main challenges in the cybersecurity field. They pose a special threat to people’s and organization’s assets by combining smartly social and technical elements. Understanding and modeling phishing attacks are part

of the solution. However, current models present a number of limitations due to their lack of ontological foundations, such as informality and unintended instances. With the aid of the *Reference Ontology for Security Engineering* (ROSE), which is based on the *Common Ontology of Value and Risk* (COVER) and the *Unified Foundational Ontology* (UFO), we propose the first well-founded *Phishing Attack Ontology* (PHATO). We have shown that PHATO represents the key elements of phishing attacks found in the research literature. We also discussed some implications of PHATO for the design of anti-phishing countermeasures.

However, PHATO, naturally, needs further validation, such as web semantic applications, expert assessment, formal validation, integration of datasets, and others. Furthermore, integrating PHATO with a *competence ontology* [33, 34, 35] can improve its capability of modeling human factors involved in phishing attacks and countermeasures. For example, competencies as types of MENTAL ATTITUDES that counteract TARGET'S FRAGILITIES: critical thinking, cybersecurity knowledge and skills, etc. Because these competencies often emerge from the interaction of other MENTAL ATTITUDES, a *system core ontology* [36] can come in handy. We intend to continue this work in this direction in the future.

Acknowledgments

Work supported by Accenture Israel Cybersecurity Labs.

References

- [1] Z. Wang, L. Sun, H. Zhu, Defining social engineering in cybersecurity, *IEEE Access* 8 (2020) 85094–85115.
- [2] Internet Crime Complaint Center, Internet Crime Report, Technical Report, Federal Bureau of Investigation of The United States of America, 2022. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
- [3] S.-S. Tseng, C.-H. Ku, T.-J. Lee, G.-G. Geng, Y.-J. Wang, Building a frame-based anti-phishing model based on phishing ontology, in: *International Conference on Advances in Information Technology*, 2013.
- [4] I. Alshanfari, R. Ismail, N. J. M. Zaizi, F. A. Wahid, Ontology-based formal specifications for social engineering, *International Journal of Technology Management and Information System* 2 (2020) 35–46.
- [5] Z. Wang, H. Zhu, P. Liu, L. Sun, Social engineering in cybersecurity: a domain ontology and knowledge graph application examples, *Cybersecurity* 4 (2021) 1–21.
- [6] F. Tchakounté, D. Molengar, J. M. Ngossaha, A description logic ontology for email phishing, *International Journal of Information Security Science* 9 (2020) 44–63.
- [7] F. Mouton, L. Leenen, M. M. Malan, H. Venter, Towards an ontological model defining the social engineering domain, in: *ICT and Society: 11th IFIP TC 9 International Conference on Human Choice and Computers, HCC11 2014, Turku, Finland, July 30–August 1, 2014. Proceedings* 11, Springer, 2014, pp. 266–279.
- [8] T. Li, X. Wang, Y. Ni, Aligning social concerns with information system security: A fundamental ontology for social engineering, *Information Systems* 104 (2022) 101699.

- [9] Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan, Phishing attacks: A recent comprehensive study and a new anatomy, *Frontiers in Computer Science* 3 (2021) 563060.
- [10] E. E. Lastdrager, Achieving a consensual definition of phishing based on a systematic review of the literature, *Crime Science* 3 (2014) 1–10.
- [11] G. Guizzardi, Ontology, ontologies and the "I" of FAIR, *Data Intelligence* 2 (2020) 181–191.
- [12] G. Guizzardi, The role of foundational ontologies for conceptual modeling and domain ontology representation, in: 7th Intl. Baltic Conf. on Databases and Information Systems, IEEE, 2006, pp. 17–25.
- [13] S. Schulz, The role of foundational ontologies for preventing bad ontology design, in: 4th Joint Ontology Workshops (JOWO), volume 2205, CEUR-WS, 2018.
- [14] C. M. Keet, The use of foundational ontologies in ontology development: an empirical assessment, in: ESWC, Springer, 2011, pp. 321–335.
- [15] Í. Oliveira, G. Engelberg, P. P. F. Barcelos, T. P. Sales, M. Fumagalli, R. Baratella, D. Klein, G. Guizzardi, Boosting D3FEND: Ontological analysis and recommendations, in: Formal Ontology in Information Systems: Proceedings of the Thirteenth International Conference (FOIS 2023), volume forthcoming, IOS Press, 2023.
- [16] Í. Oliveira, T. P. Sales, R. Baratella, M. Fumagalli, G. Guizzardi, An ontology of security from a risk treatment perspective, in: International conference on conceptual modeling, Springer, 2022, pp. 365–379.
- [17] T. P. Sales, F. Baião, G. Guizzardi, J. P. A. Almeida, N. Guarino, J. Mylopoulos, The common ontology of value and risk, in: Conceptual Modeling. ER 2018, volume 11157, Springer, 2018, pp. 121–135.
- [18] G. Guizzardi, A. Botti Benevides, C. M. Fonseca, D. Porello, J. P. A. Almeida, T. P. Sales, Ufo: Unified foundational ontology, *Applied ontology* 17 (2022) 1–44.
- [19] F. Salahdine, N. Kaabouch, Social engineering attacks: A survey, *Future internet* 11 (2019).
- [20] K. L. Chiew, K. S. C. Yong, C. L. Tan, A survey of phishing attacks: Their types, vectors and technical approaches, *Expert Systems with Applications* 106 (2018) 1–20.
- [21] M. Jakobsson, Modeling and preventing phishing attacks, in: *Financial Cryptography*, volume 5, Citeseer, 2005.
- [22] J. Hong, The state of phishing attacks, *Commun. ACM* 55 (2012) 74–81. URL: <https://doi.org/10.1145/2063176.2063197>. doi:10.1145/2063176.2063197.
- [23] Z. Wang, H. Zhu, L. Sun, Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods, *IEEE Access* 9 (2021) 11895–11910.
- [24] M. Jakobsson, S. Myers, Phishing and countermeasures: understanding the increasing problem of electronic identity theft, John Wiley & Sons, 2006.
- [25] G. Guizzardi, et al., Towards ontological foundations for conceptual modeling: The Unified Foundational Ontology (UFO) story, *Applied ontology* 10 (2015) 259–271.
- [26] M. Verdonck, F. Gailly, Insights on the use and application of ontology and conceptual modeling languages in ontology-driven conceptual modeling, in: Intl. Conf. on Conceptual Modeling, Springer, 2016, pp. 83–97.
- [27] R. Baratella, et al., Understanding and modeling prevention, in: Research Challenges in Information Science. RCIS 2022, volume 389–405, Springer, 2022, pp. 389–405.
- [28] G. Guizzardi, et al., Grounding software domain ontologies in the Unified Foundational Ontology (UFO): The case of the ODE software process ontology., in: Ibero-American

- Conference on Software Engineering, 2008, pp. 127–140.
- [29] K. Jansson, R. von Solms, Phishing for phishing awareness, *Behaviour & information technology* 32 (2013) 584–593.
 - [30] Í. Oliveira, et al., How FAIR are security core ontologies? A systematic mapping study, in: *Research Challenges in Information Science.*, 2021, pp. 107–123.
 - [31] B. F. Martins, et al., Conceptual characterization of cybersecurity ontologies, in: *IFIP Working Conference on The Practice of Enterprise Modeling*, Springer, 2020, pp. 323–338.
 - [32] B. F. Martins, et al., A framework for conceptual characterization of ontologies and its application in the cybersecurity domain, *Software and Systems Modeling* 21 (2022) 1437–1464.
 - [33] R. F. Calhau, C. L. B. Azevedo, J. P. A. Almeida, Towards Ontology-based Competence Modeling in Enterprise Architecture, in: *25th IEEE Int. EDOC Conference (EDOC 2021)*, IEEE, 2021. doi:10.1109/edoc52215.2021.00018.
 - [34] R. F. Calhau, J. P. A. Almeida, Zooming in on competences in ontology-based enterprise architecture modeling, in: *2022 IEEE 26th International Enterprise Distributed Object Computing Workshop (EDOCW)*, 2022.
 - [35] R. F. Calhau, S. Kokkula, D. Cameron, G. Guizzardi, J. P. A. Almeida, Modeling competence framework elements with an ontology-based approach, in: *2023 IEEE 25th Conference on Business Informatics (CBI)*, IEEE, 2023. URL: <https://doi.org/10.1109/cbi58679.2023.10187498>. doi:10.1109/cbi58679.2023.10187498.
 - [36] R. F. Calhau, T. P. Sales, Í. Oliveira, S. Kokkula, L. F. Pires, D. Cameron, G. Guizzardi, J. P. A. Almeida, A system core ontology for capability emergence modeling, in: *27th IEEE Int. EDOC Conference (EDOC 2023)*, IEEE, 2023.