Toward a Phishing Attack Ontology

Ítalo Oliveira[1,2], Rodrigo F. Calhau[2,3], Giancarlo Guizzardi[2,4]

[1]Free University of Bozen-Bolzano, Bolzano, Italy

[2]University of Twente, Enschede, The Netherlands

[3]Federal University of Espírito Santo, Vitória, Brazil

[4]Stockholm University, Stockholm, Sweden

My webpage: `https://italojsoliveira.github.io`

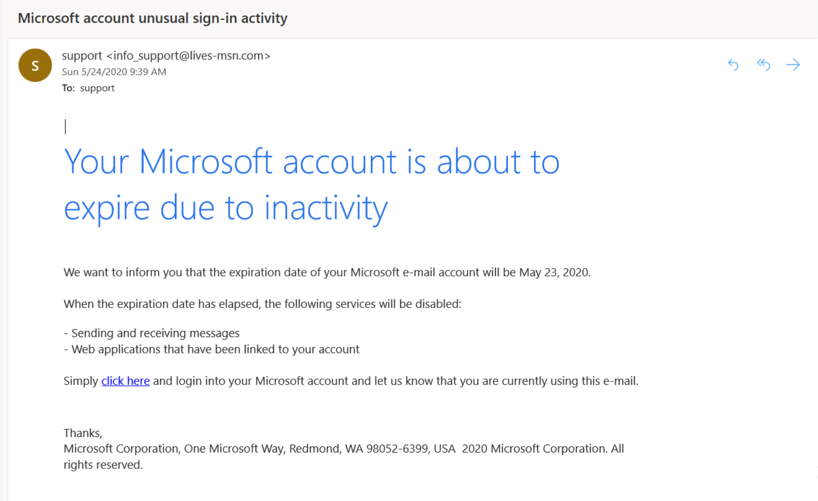
Content

Problem: Understanding and Modeling Phishing Attacks

Ontological Foundations: Value, Risk, and Security

A Phishing Attack Ontology (PHATO)

Future Directions



Microsoft account unusual sign-in activity

support <info_support@lives-msn.com>
Sun 5/24/2020 9:39 AM
To: support

Your Microsoft account is about to expire due to inactivity

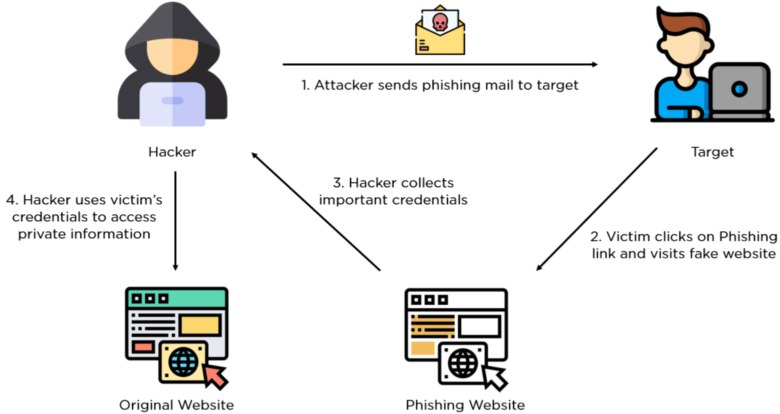
We want to inform you that the expiration date of your Microsoft e-mail account will be May 23, 2020.

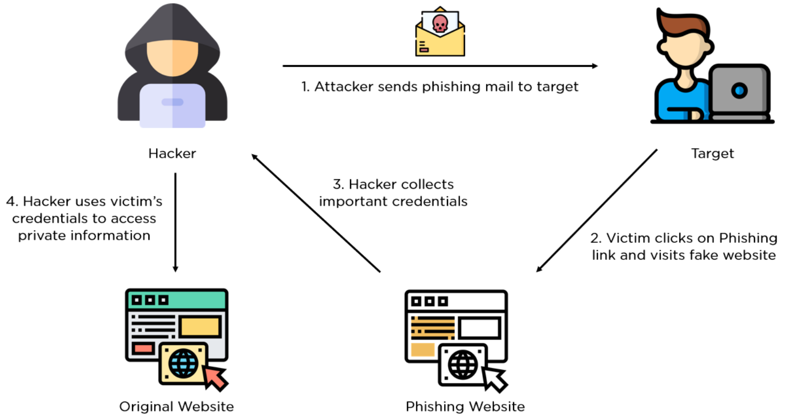
When the expiration date has elapsed, the following services will be disabled:

- Sending and receiving messages
- Web applications that have been linked to your account

Simply click here and login into your Microsoft account and let us know that you are currently using this e-mail.

Thanks,
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA 2020 Microsoft Corporation. All rights reserved.

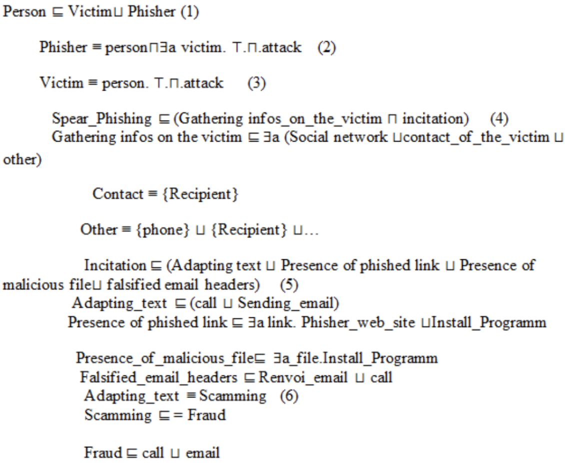

Hacker
1. Attacker sends phishing mail to target
Target
4. Hacker uses victim's credentials to access private information
3. Hacker collects important credentials
2. Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website



1. Attacker sends phishing mail to target
Hacker
Target
4. Hacker uses victim's credentials to access private information
3. Hacker collects important credentials
2. Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

"scalable act of deception whereby impersonation is used to obtain information from a target"

A description logic/OWL ontology of phishing attacks



Person $\sqsubseteq$ Victim$\sqcup$ Phisher (1)

Phisher $\equiv$ person$\sqcap\exists$a victim. $\top.\sqcap$.attack (2)

Victim $\equiv$ person. $\top.\sqcap$.attack (3)

Spear_Phishing $\sqsubseteq$ (Gathering infos_on_the_victim $\sqcap$ incitation) (4)
Gathering infos on the victim $\sqsubseteq\exists$a (Social network $\sqcup$contact_of_the_victim $\sqcup$
other)

Contact $\equiv$ {Recipient}

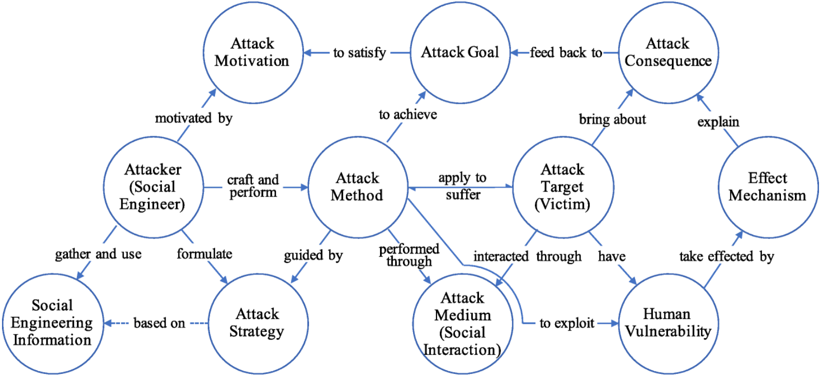
Other $\equiv$ {phone} $\sqcup$ {Recipient} $\sqcup$…

Incitation $\sqsubseteq$ (Adapting text $\sqcup$ Presence of phished link $\sqcup$ Presence of
malicious file$\sqcup$ falsified email headers) (5)
Adapting_text $\sqsubseteq$ (call $\sqcup$ Sending_email)
Presence of phished link $\sqsubseteq\exists$a link. Phisher_web_site $\sqcup$Install_Programm

Presence_of_malicious_file$\sqsubseteq$ $\exists$a_file.Install_Programm
Falsified_email_headers $\sqsubseteq$Renvoi_email $\sqcup$ call
Adapting_text $\equiv$Scamming (6)
Scamming $\sqsubseteq$= Fraud

Fraud $\sqsubseteq$ call $\sqcup$ email

A domain ontology of social engineering in cybersecurity



- It is well-known that ontological foundations support the development of conceptual models (consistent, interoperable, more appropriate, etc.) 🤩

- It is well-known that ontological foundations support the development of conceptual models (consistent, interoperable, more appropriate, etc.) 🤩
- Still, in academia and industry, people often develop conceptual models from scratch. 🤷

- It is well-known that ontological foundations support the development of conceptual models (consistent, interoperable, more appropriate, etc.) 🤩
- Still, in academia and industry, people often develop conceptual models from scratch. 🤷
- What if we could develop an ontologically well-founded conceptual model for phishing attacks? 🤔

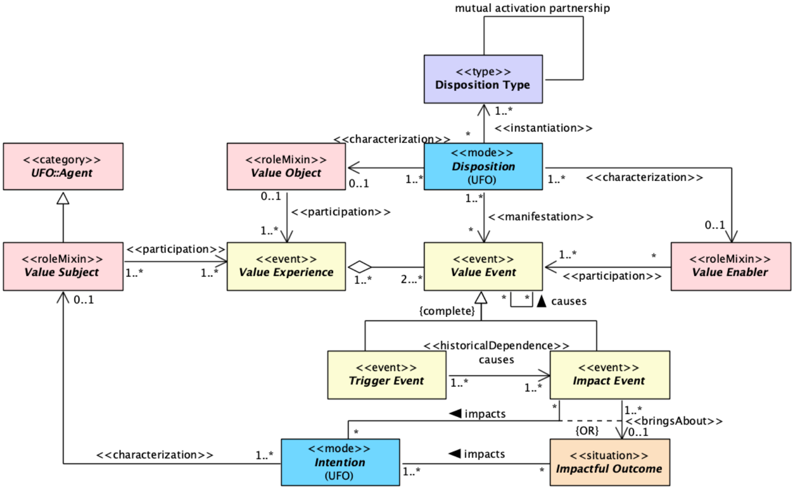
Unified Foundational Ontology

ONTOUML

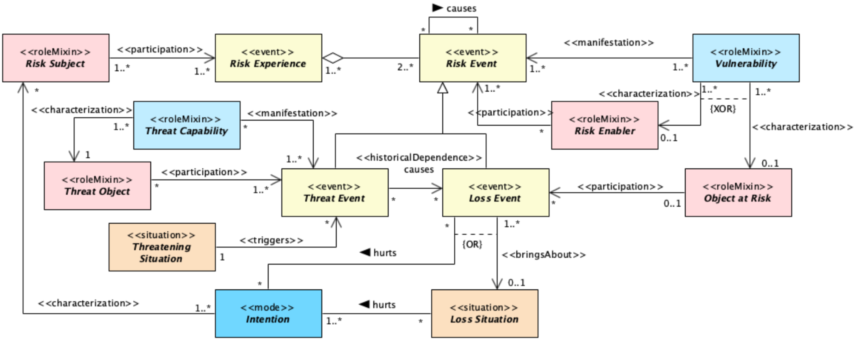
Common Ontology of Value and Risk

Reference Ontology for Security Engineering

Value Experience🤑



Risk Experience😱



<<roleMixin>> *Risk Subject*

<<event>> *Risk Experience*

<<event>> *Risk Event*

<<roleMixin>> *Vulnerability*

<<roleMixin>> *Threat Capability*

<<roleMixin>> *Risk Enabler*

<<roleMixin>> *Threat Object*

<<event>> *Threat Event*

<<event>> *Loss Event*

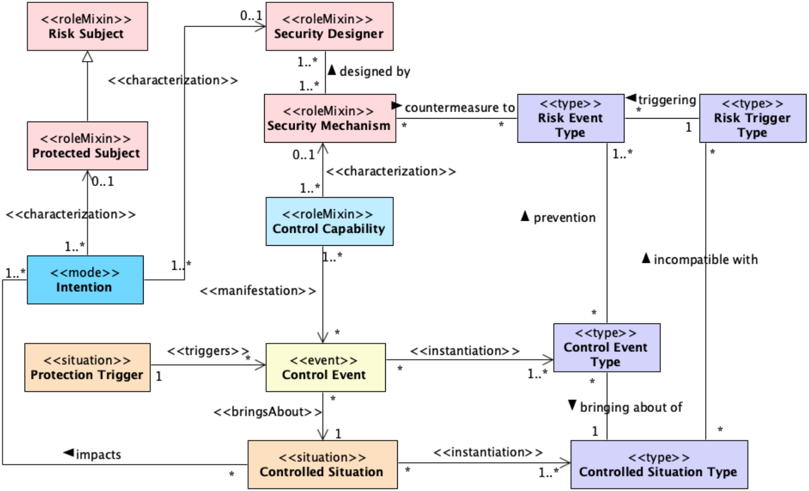
<<roleMixin>> *Object at Risk*

<<situation>> *Threatening Situation*

<<mode>> *Intention*

<<situation>> *Loss Situation*

Security Mechanism



A Phishing Attack Ontology (PHATO)🎣

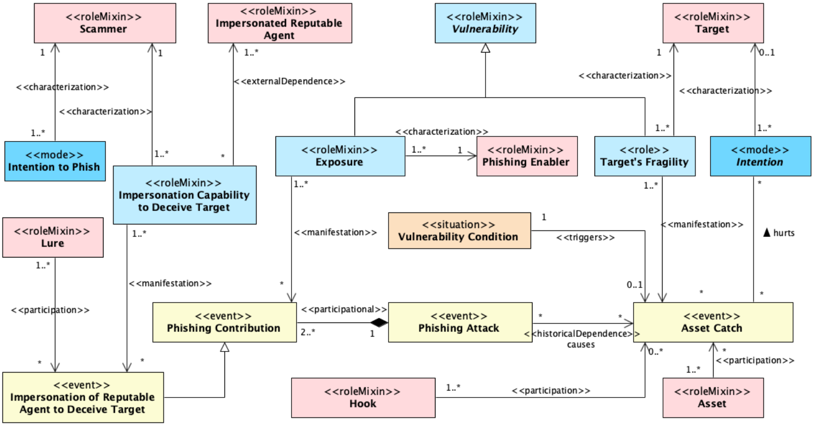
- *phato*, in Portuguese, can sound like “fato” (*fact*) or “pato” (*duck*) - Brazilian slang for gullible, naive person. 🙈

A Phishing Attack Ontology (PHATO)🎣

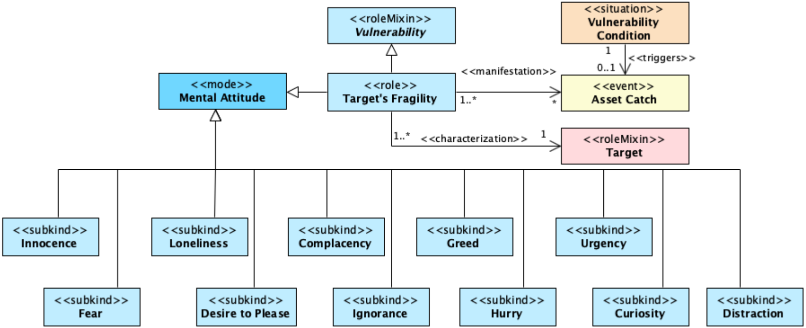
- *phato*, in Portuguese, can sound like “fato” (*fact*) or “pato” (*duck*) - Brazilian slang for gullible, naive person. 🙈

- Our approach involves *specializing* the ontologies of value, risk, and security in phishing domain-specific concepts.

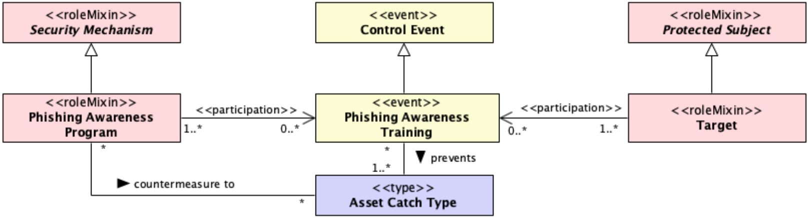
A Model for Phishing Attacks🧐



Several Target's Fragilities🤒



Counteracting Phishing Attacks by Phishing Awareness Program🧑‍💻



All related files of PHATO can be found at:

`https://github.com/utwente-scs/phishing-ontology`

Future Work

- Web semantic applications thanks to gUFO implementation.

Future Work

- Web semantic applications thanks to gUFO implementation.
- Expert assessment.

Future Work

- Web semantic applications thanks to gUFO implementation.
- Expert assessment.
- Formal validation (Alloy Analyzer).

Future Work

- Web semantic applications thanks to gUFO implementation.
- Expert assessment.
- Formal validation (Alloy Analyzer).
- Integration of datasets.

Future Work

- Web semantic applications thanks to gUFO implementation.
- Expert assessment.
- Formal validation (Alloy Analyzer).
- Integration of datasets.
- Competence Ontology.

Future Work

- Web semantic applications thanks to gUFO implementation.
- Expert assessment.
- Formal validation (Alloy Analyzer).
- Integration of datasets.
- Competence Ontology.
- System Core Ontology (*emergent* mental attitudes).

Thank you! Questions?

Get in touch: 😇

- i.j.dasilvaoliveira@utwente.nl
- `https://italojsoliveira.github.io`
- Semantics, Cybersecurity, and Services Group: `https://www.utwente.nl/en/eemcs/scs/`