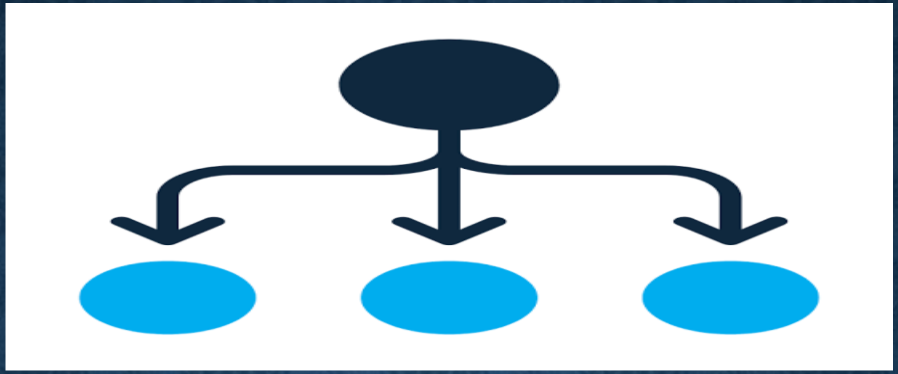
University of the Western Cape



ONTOLOGY

TOPIC: PHISHING ONTOLOGY FOR MALICIOUS EMAILS

XAKA YAMKELA

3538718

SUPERVISOR: PROFFESOR LOUISE LEENEN

COMPUTER SCIENCE(HONS)

BACKGROUND

- An ontology that is identifying if an email is a phishing or normal Email.

IMPLEMENTATION TOOLS AND RESOURCES

protégé

PHISHING QUIZ

Are you confident that you and your staff know how to spot a phishing email?

Take our quiz to find out!

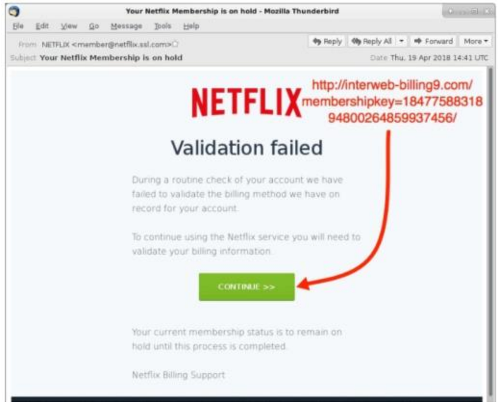
PHISHING STAFF AWARENESS

Annual e-learning subscription service

+ Quarterly updates on the latest phishing tactics

+ Free monthly staff security awareness newsletter

Subscribe now from only £15



Your Netflix Membership is on hold - Mozilla Thunderbird
File Edit View Go Message Tools Help
Reply
Reply All
Forward
More

From NETFLIX <member@netflix.ssl.com>

Subject Your Netflix Membership is on hold

Date Thu, 19 Apr 2018 14:41 UTC

NETFLIX

http://interweb-billing9.com/membershipkey=1847758831894800264859937456/

Validation failed

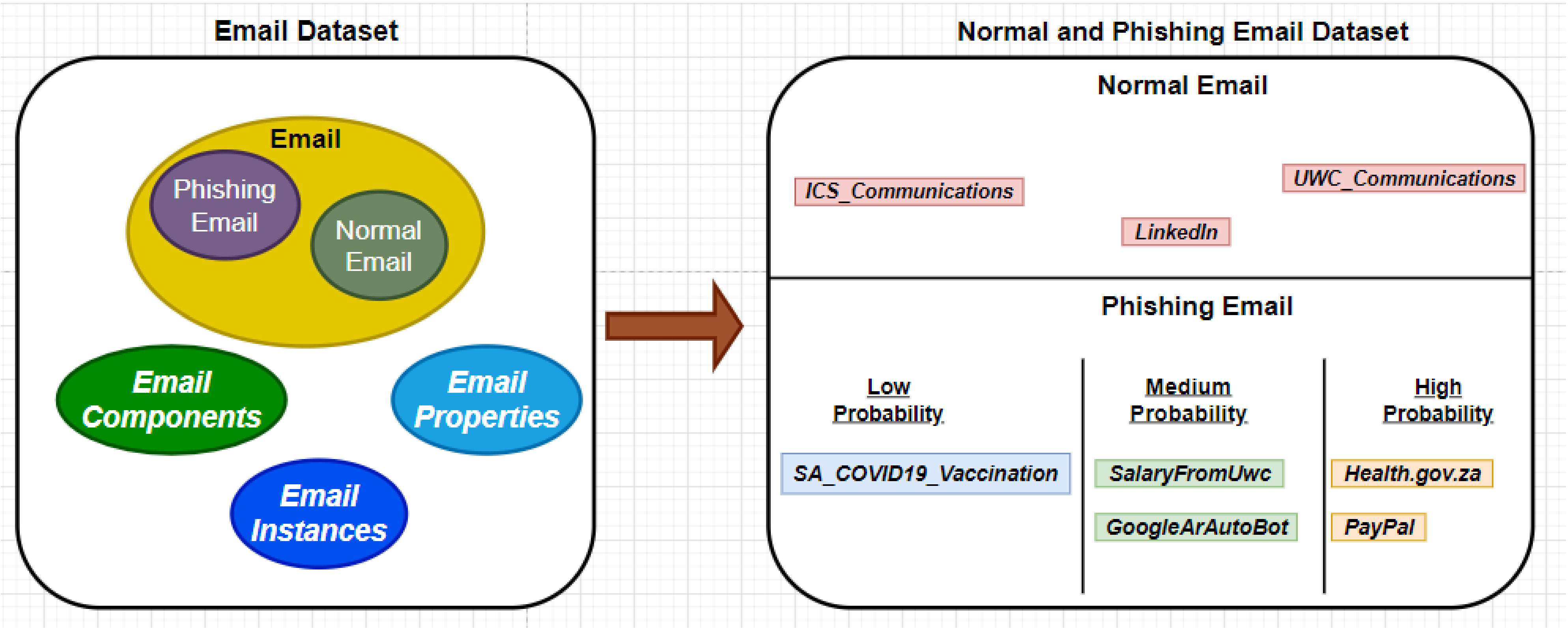
During a routine check of your account we have failed to validate the billing method we have on record for your account.

To continue using the Netflix service you will need to validate your billing information.

CONTINUE >>

Your current membership status is to remain on hold until this process is completed.

Netflix Billing Support


Email Dataset

Email

Phishing Email

Normal Email

Email Components

Email Properties

Email Instances

Normal and Phishing Email Dataset

Normal Email

ICS_Communications

UWC_Communications

LinkedIn

Phishing Email

Low Probability

SA_COVID19_Vaccination

Medium Probability

SalaryFromUwc

GoogleArAutoBot

High Probability

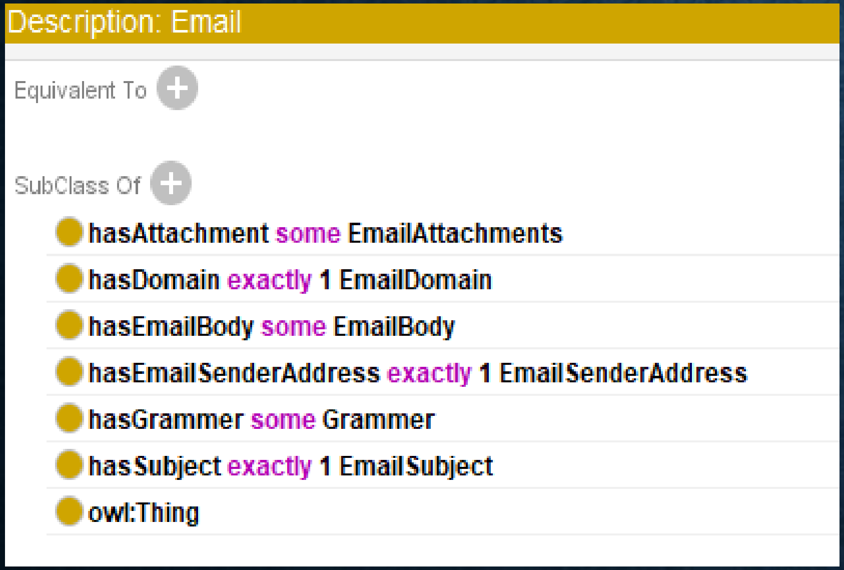
Health.gov.za

PayPal

DESIGN IMPLEMENTATION

DEFINITION OF CLASSES AND SUBCLASSES

Primitive classes



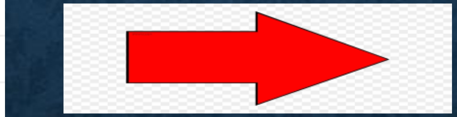
Description: Email

Equivalent To

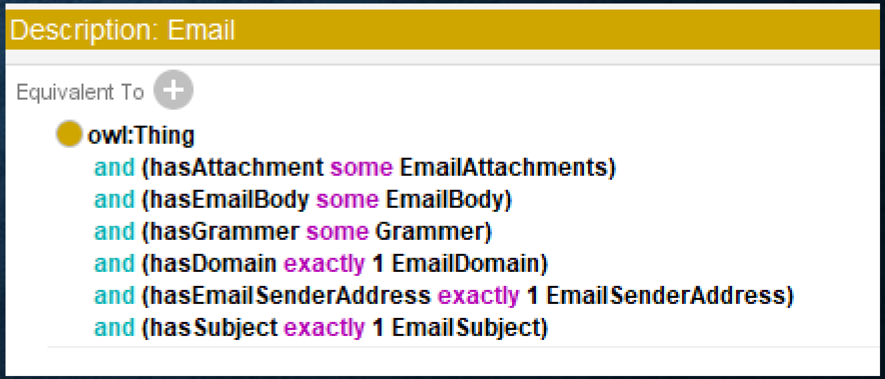
SubClass Of

- hasAttachment some EmailAttachments
- hasDomain exactly 1 EmailDomain
- hasEmailBody some EmailBody
- hasEmailSenderAddress exactly 1 EmailSenderAddress
- hasGrammer some Grammer
- hasSubject exactly 1 EmailSubject
- owl:Thing

Converted



Defined classes

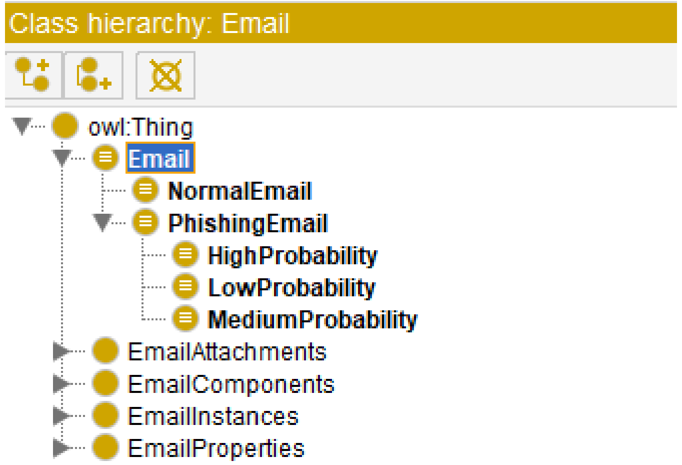


Description: Email

Equivalent To

```
owl:Thing
 and (hasAttachment some EmailAttachments)
 and (hasEmailBody some EmailBody)
 and (hasGrammer some Grammer)
 and (hasDomain exactly 1 EmailDomain)
 and (hasEmailSenderAddress exactly 1 EmailSenderAddress)
 and (hasSubject exactly 1 EmailSubject)
```

CLASS HIERARCHY FOR ASSERTED AND INFERRED CLASSES

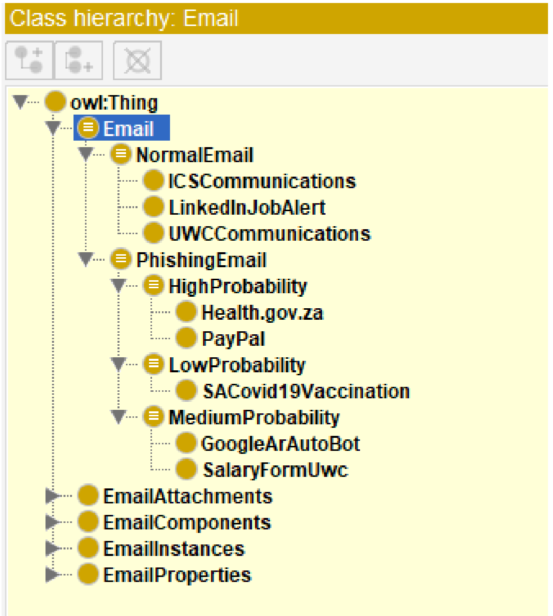


Class hierarchy: Email

```
owl:Thing
  Email
    NormalEmail
    PhishingEmail
      HighProbability
      LowProbability
      MediumProbability
  EmailAttachments
  EmailComponents
  EmailInstances
  EmailProperties
```

Before the Reasoner is Executed

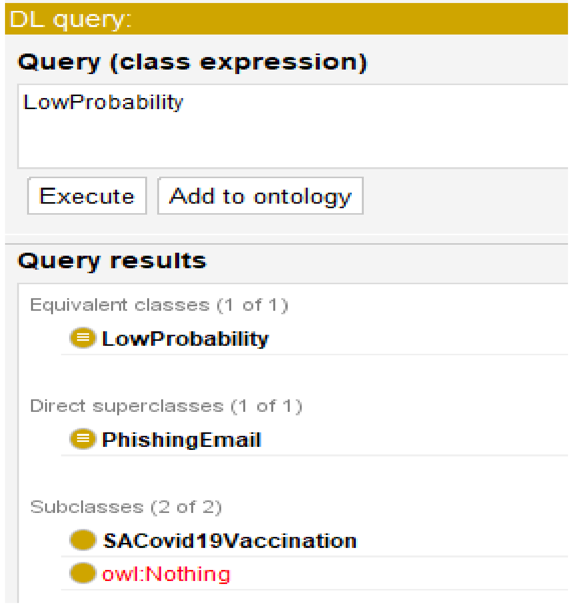
After the Reasoner is Executed



Class hierarchy: Email

```
owl:Thing
  Email
    NormalEmail
      ICSCommunications
      LinkedInJobAlert
      UWCCommunications
    PhishingEmail
      HighProbability
        Health.gov.za
        PayPal
      LowProbability
        SACovid19Vaccination
      MediumProbability
        GoogleArAutoBot
        SalaryFormUwc
  EmailAttachments
  EmailComponents
  EmailInstances
  EmailProperties
```

Low Probability



Query (class expression)

LowProbability

Query results

Equivalent classes (1 of 1)

- LowProbability

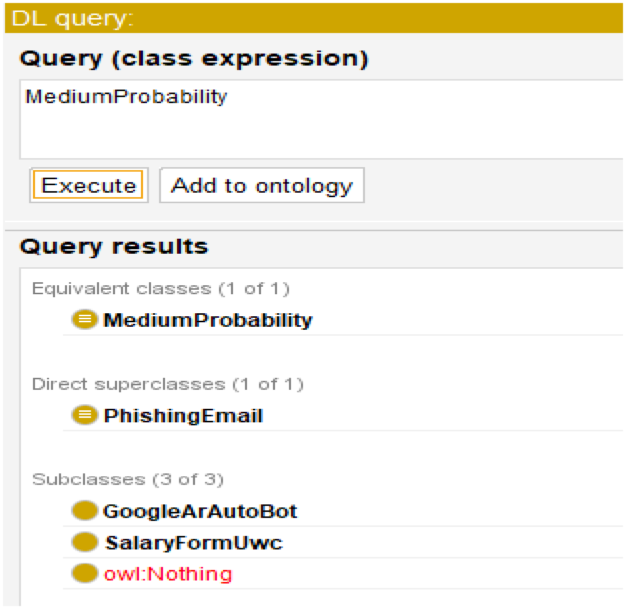
Direct superclasses (1 of 1)

- PhishingEmail

Subclasses (2 of 2)

- SACovid19Vaccination
- owl:Nothing

Medium Probability



Query (class expression)

MediumProbability

Query results

Equivalent classes (1 of 1)

- MediumProbability

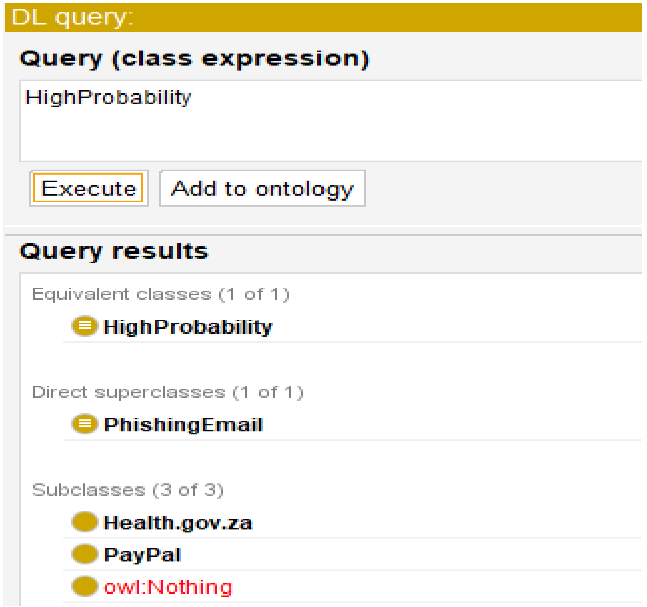
Direct superclasses (1 of 1)

- PhishingEmail

Subclasses (3 of 3)

- GoogleArAutoBot
- SalaryFormUwc
- owl:Nothing

High Probability



Query (class expression)

HighProbability

Query results

Equivalent classes (1 of 1)

- HighProbability

Direct superclasses (1 of 1)

- PhishingEmail

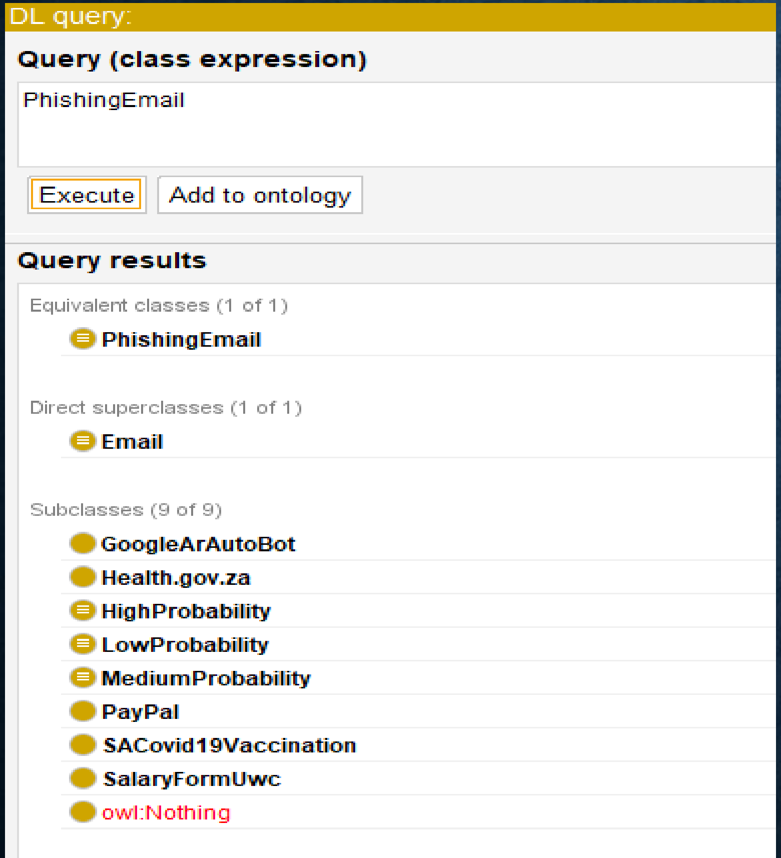
Subclasses (3 of 3)

- Health.gov.za
- PayPal
- owl:Nothing

DL QUERY FOR LOW MEDIUM AND HIGH PROBABILITY

QUERIES (CONT..)

Phishing emails



DL query:

Query (class expression)

PhishingEmail

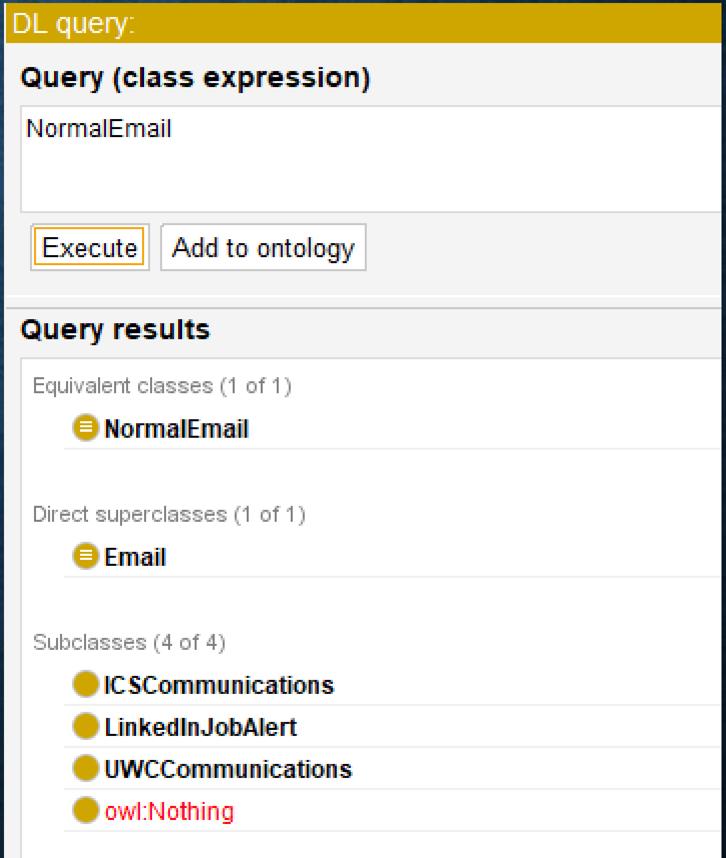
Query results

Equivalent classes (1 of 1)
- PhishingEmail

Direct superclasses (1 of 1)
- Email

Subclasses (9 of 9)
- GoogleArAutoBot
- Health.gov.za
- HighProbability
- LowProbability
- MediumProbability
- PayPal
- SACovid19Vaccination
- SalaryFormUwc
- owl:Nothing

Normal Emails



DL query:

Query (class expression)

NormalEmail

Query results

Equivalent classes (1 of 1)
- NormalEmail

Direct superclasses (1 of 1)
- Email

Subclasses (4 of 4)
- ICSCommunications
- LinkedInJobAlert
- UWCCommunications
- owl:Nothing

REFERENCES

- [1] A. Vedeshin, “Contributions Of Understanding And Defending Against Social Engineering Attacks,” 2016.
- [2] “The 5 most common types of phishing attack - IT Governance Blog En.” [Online]. Available: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack. [Accessed: 06-Jun-2020].
- [3] “When Phishing Starts from the Inside -.” [Online]. Available: https://blog.trendmicro.com/phishing-starts-inside/. [Accessed: 06-Jun-2020].
- [4] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, “Towards an Ontological Model Defining,” *IFIP Int. Conf. Hum. Choice Comput.*, pp. 266–279, 2014.

THANK YOU.