Phishing and PhyFinder

Ryan Yoak

Phishing Emails

Phishing emails are emails that attempt to gain information about the target that can be used to help some end.

They employ a number of techniques in an attempt to achieve this

- Banking information
- Passwords
- Identity
- Ect.

Phishing Today

- In 2019 $57,000,000 was lost to fishing emails according to the FTC
- Each day 1000s of new phishing email attacks are launched
- FBI's Internet Crime Complaint Center receives 1300 complaints every day and billions in losses

Techniques used in Phishing Emails

- Spelling errors
- Specific stories
- Links to suspicious websites
- Evocative language
- Claiming to be people they are not

Phyfinder

- Phyfinder is a python module that attempts to classify emails based on how likely it feels they are one based on a number of factors.
- It looks at several parts of an email such as
  - Spelling
  - Use of evocative language
  - Links and their destinations
  - Addresses and the company names used
  - History of the address
  - Addresses existence in lists of trusted/benign addresses

PhyFinder Class

```
 9  class PhyFinder:
10      def __init__ (self, trusted_addresses, malicious_addresses, user_name):
11          self.trusted_addresses = trusted_addresses
12          self.malicious_addresses = malicious_addresses
13          self.user_name = user_name
14          self.suspicious_phrases = urgentPhrases
15          self.suspicious_addresses = {}
16          self.use_suspicious_addresses = True
```

The PhyFinder class is implemented by an Inbox Class that passes each piece of mail it receives into the PhyFinder class to assign it a score from 0 – 100 based on how likely it thinks it is a phishing email

Inbox and Mail Classes

```
7   class Inbox:
8       def __init__ (self, trusted_addresses, malicious_addresses, user_name):
9           self.Mechanism = PhyFinder(trusted_addresses, malicious_addresses, user_name)
10          self.inbox = []
11          self.spam = []
12          self.threshold = 51
13          self.spam_since_last_checked = 0
```

```
3   class Mail:
4       def __init__(self, address, subject, body, time, attachments):
5           self.address = address
6           self.subject = subject
7           self.body = body
8           self.time = time
9           self.attachments = attachments
10          self.read = False
11          self.checked = False
12          self.phishing = 0
```

PhyPhinder Methods

```
 9  class PhyFinder:
10      def __init__ (self, trusted_addresses, malicious_addresses, user_name):⋯
17
18      def spellCheck(self, header, body):⋯
45
46      def linkChecker(self, body):⋯
67
68      def phrasesChecker(self, header, body):⋯
84
 5      def addressChecker(self, address, header, body):⋯
93
94      def checkMail(self, mail, threshold):⋯
```

Title Lorem Ipsum

Dolor Sit Amet

Consectetuer Elit

Nunc Viverra

Pellentesque Habitant

Lorem Ipsum

Dolor Sit Amet

Consectetuer Elit

Nunc Viverra

Pellentesque Habitant

Lorem Ipsum