Inferring Phishing Intention via Webpage Appearance and Dynamics: A Deep Vision Based Approach

Ruofan Liu, Yun Lin*, Xianglin Yang, Siang Hwee Ng, Dinil Mon Divakaran, Jin Song Dong

Presenter: Yun Lin
National University of Singapore
(Research Assistant Professor)
Shanghai Jiao Tong University
(incoming Associate Professor)
Phishing Attack
Phishing Attack

Phishing site

login credential, bank account, ...

Lin, Yun | Research Assistant Professor | NUS 3
Phishing Attack

- transfer money
- deliver misinformation
- start new attacks (e.g., deploying trojan)

Phishing site

login credential, bank account, ...
At least S$8.5 million lost in December to phishing scams involving OCBC Bank.

Police warn of banking-related phishing scams; S$114,000 lost since May.

At least S$12,500 lost this month to Netflix phishing scams.

At least five victims have fallen prey to the phishing scams since the beginning of July, said the police.
Phishing Attacks Rose 61% in 2022, New Study Finds

Monthly number of phishing attacks reported more than doubled since 1 May 2020
Cat-and-mouse Game

Google Safe Browsing

Blacklist

abc.com
Cat-and-mouse Game

~7 days

Google Safe Browsing

Blacklist

abc.com

abc.com
Cat-and-mouse Game

~7 days

abc.com efg.com

Google Safe Browsing

Blacklist

abc.com
Cat-and-mouse Game

Full Automation

Google Safe Browsing

Blacklist

abc.com  efg.com  ...  xyz.com

Update every week
Cat-and-mouse Game

Evolving HTML code

abc.com efg.com ... xyz.com
PhishIntention Solution

- **brand intention**
- **credential-taking intention**

abc.com

PI (PhishIntention)

look
PhishIntention Solution

- **brand intention**
- **credential-taking intention**
- **consistency checking**

abc.com

PI (PhishIntention)
PhishIntention Solution

Take care of you and yours at home, and we can take care of you online.

Sign Up Now

credential-taking intention

interact

PI (PhishIntention)
Reference-based Phishing Detection

Domain

- facebook.com
- paypal.com

Representation

...
Reference-based Phishing Detection

facebook.com (domain)
match

abc.com

Phishing Alarm
Representation as Screenshot (VisualPhishNet, CCS 2020)

Reference | Benign Webpage | Phishing Webpage
--- | --- | ---
false positive (similar screenshot)
Representation as Screenshot (VisualPhishNet, CCS 2020)

Reference

Benign Webpage

Phishing Webpage

false negative (dissimilar screenshot)
Representation as Logo (Phishpedia, USENIX Security 2021)

false positive

Benign Webpage
The screenshot and logo can only convey partial webpage intention.
PhishIntention Solution

- Comprehensive Intention
- Static and Dynamic Webpage Analysis
Step 1: Extract the Abstract Webpage Layout (AWL)
As an object detection task:

Step 1: Extract the Abstract Webpage Layout (AWL)
Step 2: Detecting Brand Intention
As a metric learning task:

Step 2: Detecting Brand Intention
Step 3: Credential-taking Intention Classification

(whether this page takes credential?)
Step 4: CRP (Credential-requiring Page) transition location
(Whether any link/button on this webpage can link to a CRP?)
Step 4: CRP (Credential-requiring Page) transition location
(Whether any link/button on this webpage can link to a CRP?)
Webpage Representation Extraction

Brand Recognition

Credential-taking Intention Recognition

Credential-taking Intention Confirmation

Webpage Screenshot

Detected Non-CRP Layout

Detected CRP Layout

CRP transition potential

AWL Extraction

Link
Webpage Representation Extraction

Brand Recognition

Credential-taking Intention Recognition

Credential-taking Intention Confirmation

Webpage Screenshot → AWL Extraction → Detected Non-CRP Layout → Link → Detected CRP Layout
Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment
Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

Precision and recall in a collected phishing webpage dataset
Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

What is the performance to find a CRP from a non-CRP?
Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

What is the performance of each component?
Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

How robust is the each of our deep learning model?
Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

What is the performance of PI to detect zero-day phishing webpages in the wild?
Experiments

• RQ1: Phishing Detection Experiment
• RQ2: CRP Location Experiment
• RQ3: Evaluating Model-wise Performance
• RQ4: Robustness Against Adversaries
• RQ5: Phishing Discovery Experiment

What is the performance of PI to detect zero-day phishing webpages in the wild?
Phishing Discovery Experiment

- Detect phishing in the wild with a Crawling system
Phishing Discovery Experiment

- Two months starting from April 2021
- PhishIntention reports 1,942 real phishing webpages, 1,368 are zero-day phishing
Phishing Discovery Experiment

- Distribution of brands of discovered phishing webpages
  - Top five brands are Microsoft (751), Facebook (146), HSBC Bank (110), Amazon (89), and Instagram (58).
Qualitative Analysis (False Positive)
Qualitative Analysis (False Negative)

Welcome! Scan your personal QR Code to view your video message.
Takeaways

- PhishIntention: a visual reference-based phishing detection solution
  - with both brand and credential-taking intentions.
  - with interaction for confirming more credential intentions.
  - with a tool to effectively detect zero-day phishing webpages.

https://github.com/lindsey98/PhishIntention