



# 分析網路 QR Code 釣魚 與實作釣魚偵測插件

指導教授：林柏青

組員：徐怡娟、曾睿銓、鄭雅云



# Experiment Part



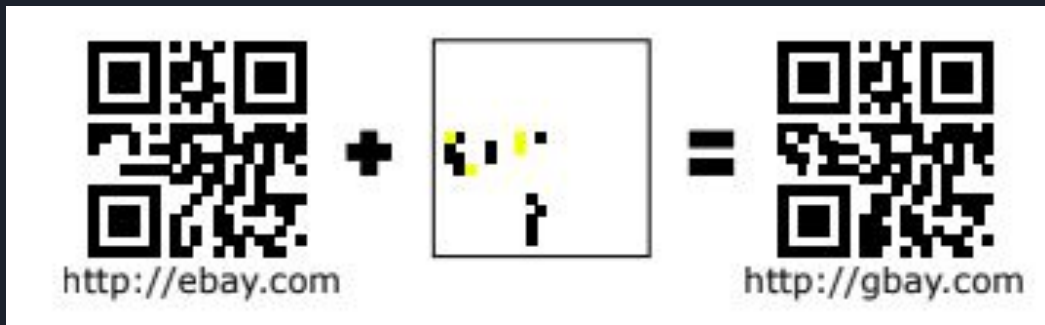
# Outline

1. Introduction
2. System Architecture
3. Experiment Settings
4. Experimental Results
5. Conclusions

# Introduction

What is QR code phishing?

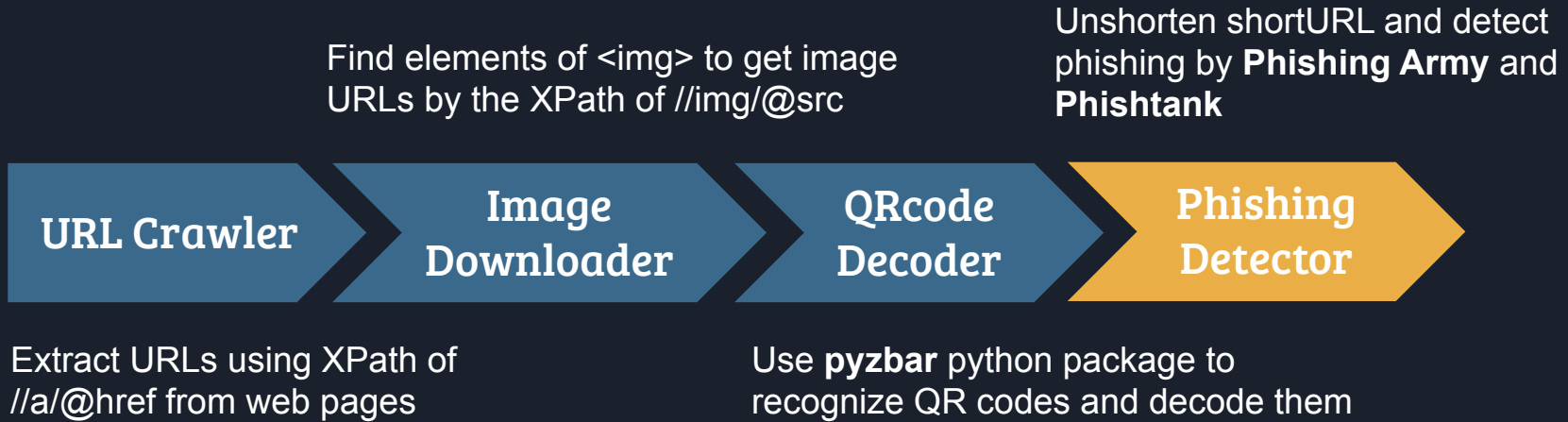
- 有利於有心人士隱藏其釣魚網址訊息
- QR code phishing is a social engineering attack aimed at getting people to hand over personal information, login credentials, or financial details. It's a lot like other forms of phishing.



A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with faint, lighter blue diagonal stripes.

# System Architecture

# System Architecture

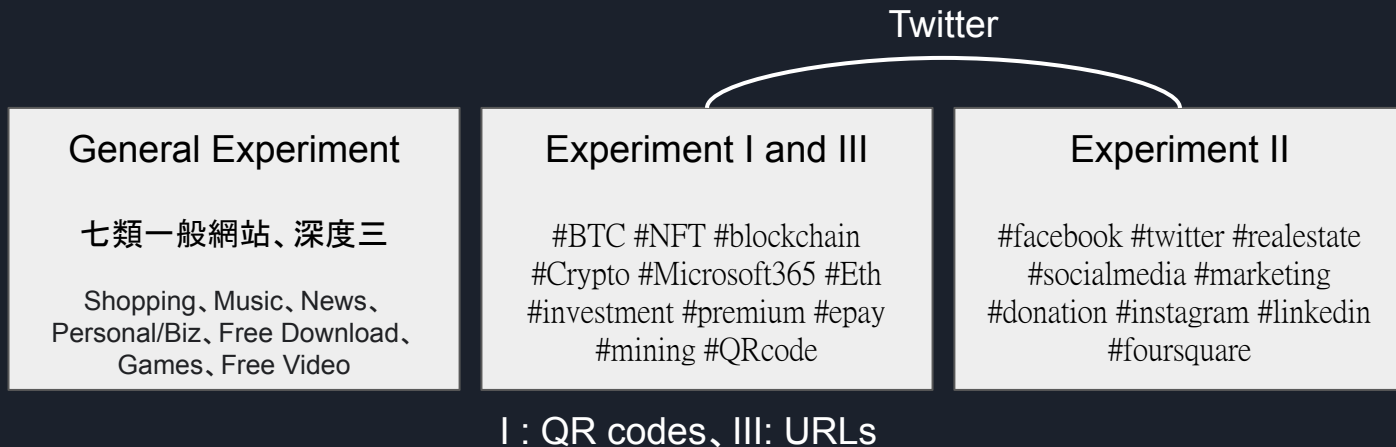




# Experiment Settings



# Experiment Settings





# Experiment Settings

1. 調查大家平常會使用的網站  
存在 QR code 釣魚的比例



# Experiment Settings

2. 使用實驗一被判定為 QR code 釣魚的文章主題標籤再做一次實驗

-> 欲透過此種方式嘗試接觸到更多 QR code 釣魚的文章



# Experiment Settings

## 3. 使用易受濫用主題標籤比較 QR code 與 URL 釣魚社交工程手法的不同





# Experimental Results

— 釣魚網址來源

# Experimental Results

2 個來自 kaywa.me  
1 個來自 urlzs.com  
1 個來自 www.sinren.com.tw

- General Experiment

Topics	URLs			Images	QR codes	Potential phishing
	In domains	Out domains	Total			
Free Download	376,722	325,761	702,493	921,833	106	0
Music	389,774	132,441	522,225	1,382,858	661	0
News	353,912	86,422	440,344	2,415,482	1,815	4
Personal/Biz	359,504	161,052	520,566	2,432,099	484	0
Free Video	872,321	2,092	874,423	1,094,566	213	0
Shopping	565,903	4,549	570,462	753,096	248	0
Games	47,569	5,919	53,498	149,000	54	0
Total	2,965,705 (80.50%)	718,236 (19.49%)	3,684,011	9,148,934	3,581	4 (0.11%)

Table 1: The number of URLs, images, QR codes, and potential phishing in different topics.

# Experimental Results

- Twitter Experiment

釣魚網址大多來自特定網域

→ 發現它們大部分是短網址工具，有些點進去後明顯是惡意網站，有些則看起來是正當營運的網站

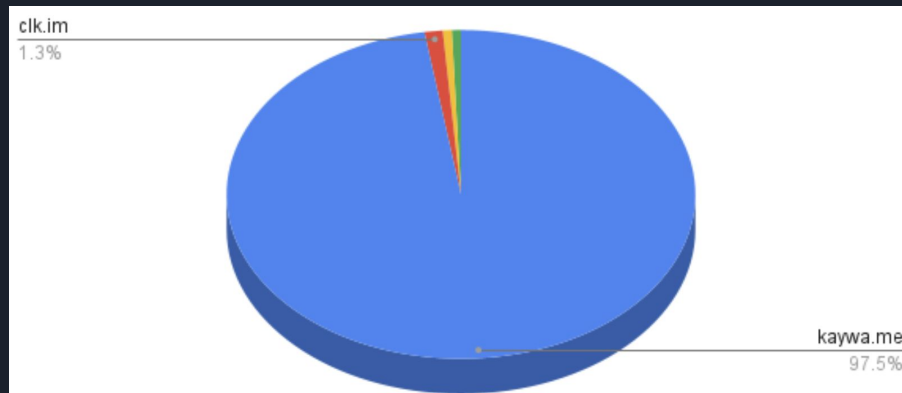


Figure 1: The percentage of domains of potential phishing QR codes in experiment I and II.

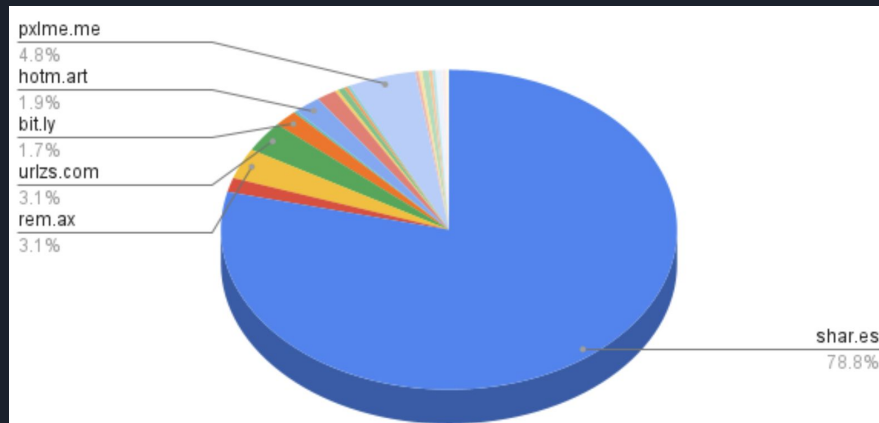


Figure 2: The percentage of domains of potential phishing URLs in experiment III.



# Experimental Results

- Twitter Experiment
  - 發現它們大部分是短網址工具，有些點進去後明顯是惡意網站，有些則看起來是正當營運的網站。
  - 某些工具本身不是惡意工具，而是在某段時間經常被有心人士濫用導致它們被納入釣魚資料庫中。
  - 存在 False positive 的原因。



# Conclusions

— 實驗數據總結





# Conclusions

1. 在 QR code 釣魚出現的比例上，一般網站為0.11%、實驗一和二分別為0.22% 和 0.28%，與 2014 年的論文中 0.15% 比例相較無明顯增加。
2. 從我們蒐集的hashtag 來看，QR code 釣魚與社群媒體主題較相關，URL 釣魚則沒有明顯的hashtag 主題。
3. 社交工程方面 QR code 與網址釣魚利用的手法類似，都是以產品推銷作為主要手法。



# Chrome Extension Part



# Outline



1. Chrome Extension Architecture
2. Demo



# Chrome Extension Architecture

## 1. 功能：

透過此 Chrome Extension 判斷當前瀏覽網頁是否有存在惡意連結

並透過自訂通知(如：Extension badge) 顯示疑似惡意連結數量

## 2. 架構：

Chrome Extension 的背景有設計監聽事件

透過 content script, 當瀏覽符合目標的連結時, 會發送通知給背景監聽事件

並依照使用者自訂, 發送通知



demo

