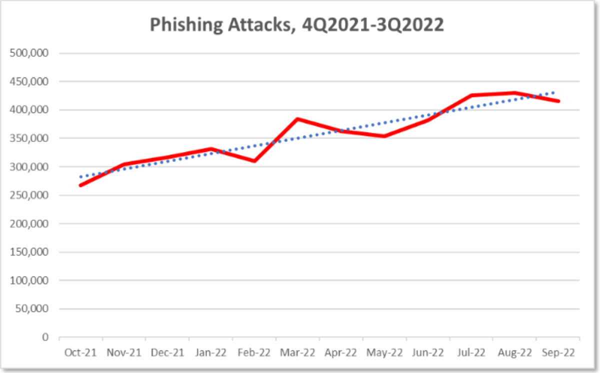
An Exploratory Study of Malicious Link Posting on Social Media Applications

Muhammad Hassan, Mahnoor Jameel, Prof. Masooda Bashir

Social Network Popularity

- Online Social Networks (OSNs) increasing popularity
  - User engagement - 72% US population was using OSNs in 2021
  - Share content, exchange messages, post life updates etc - Perception of trust
- Attackers target popularity of OSNs
  - Link-based attacks (phishing, malware, virus etc.)
  - Impersonating Financial, Employer and Business entities
  - Targeting Personally Identifiable Information *PII*, Credentials, Business Info.



APWG Report

URL Blocklisting

- Google Safe Browsing (GSB), PhishTank and VirusTotal
- These services maintains lists of known malicious and suspicious URLs.
  - Malicious URLS = Malware, Phishing, Virus, Spam etc
- Provides reports on URLs and domains’
  - Identification - monitoring user reports, web scanning, URL structure etc
- Integration of URL Blocklisting with OSN
  - Users’ protection by limiting spread of malware
  - reduce the risk cybercrime (*PII* & credential leak, identity theft etc.)

Evaluating Malicious Link Detection in OSNs

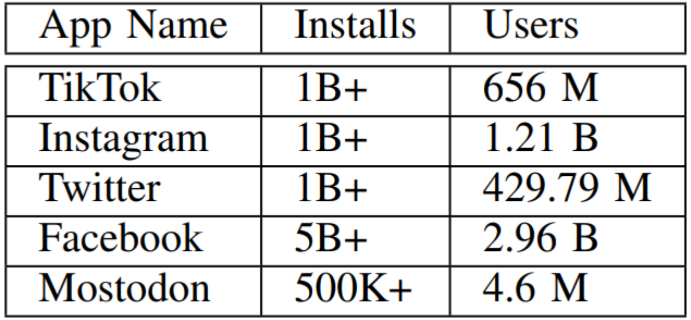
- **RQ1:** Is the user able to post a malicious link in selected social media application?

- **RQ2:** If the application block a malicious URLs, can the user bypass that security check?

Research Methodology

- Top 5 applications from *Social* category of *Google Play Store*
  - # of installation and populous user-base
- Created test accounts
  - *Pseudo(*fake*)* demographic information
- Anonymity and verification
  - *ProtonMail* was used for test accounts

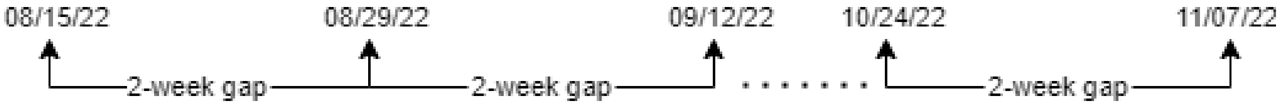
- *Ethical Consideration*
  - Limited visibility and audience



App Name	Installs	Users
TikTok	1B+	656 M
Instagram	1B+	1.21 B
Twitter	1B+	429.79 M
Facebook	5B+	2.96 B
Mostodon	500K+	4.6 M

Malicious URL Selection

- Collection: 35 malicious URLs over 3 month, sampling 5 URLs every two weeks from PhishTank database.


08/15/22

08/29/22

09/12/22

10/24/22

11/07/22

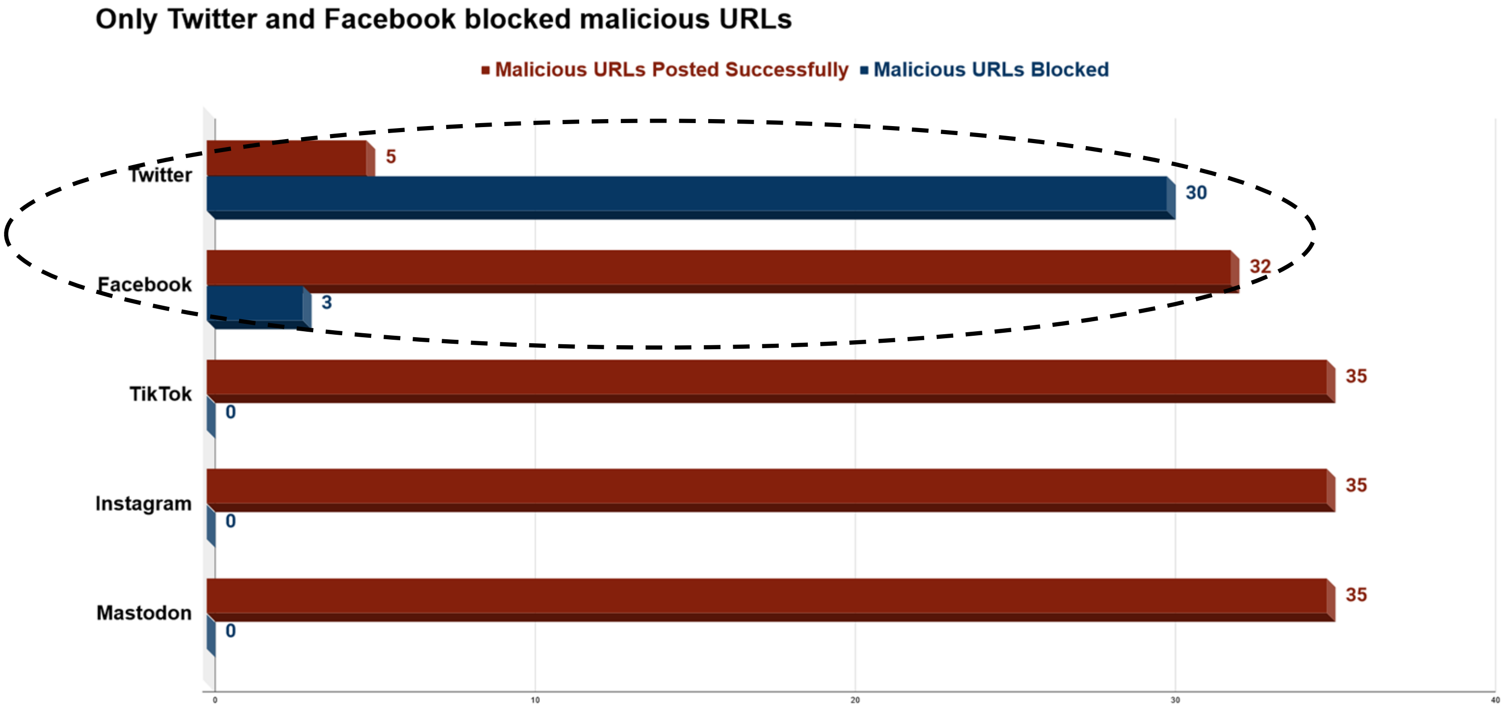
2-week gap

2-week gap

2-week gap

- Original malicious URLs (sampled from *PhishTank*) shared on app;
  - if blocked, *Redirectional link* using Tinyurl service
  - Example: *ww1.linkegin.com/* ➡ *https://tinyurl.com/damsd5w3*
- URLs shared on test account profiles
  - as direct messages on apps where text posting functionality is not present

Original Malicious URL Posting on OSN



Transformed URLs on OSNs

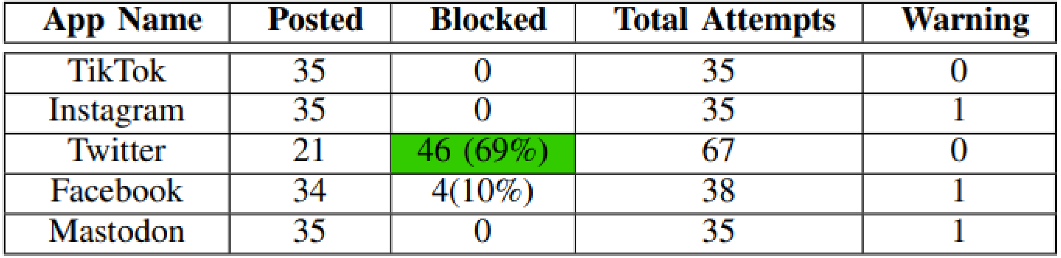
- Original malicious URLs blocked
  - Twitter: 30
  - Facebook: 3
- Transformed (Redirectional) malicious URLs results

	Redirection URLs Posted Successfully	Redirection URLs Blocked
Twitter	16	14
Facebook	2	1

Results: Posting Malicious Links

- **RQ1 - Posting Original Malicious URLs from URL Blocklists**
  - Only Twitter and Facebook blocked the original malicious URLs
  - Following showed some warning (not blocked those suspected URLs)
    - Instagram, Mastodon, and Facebook

- **RQ2 - Bypass Security against Malicious URLS**
  - Redirectional URLs has shown to help in evading security
- Only **23.8%** of the total malicious links being blocked, primarily by Twitter



App Name	Posted	Blocked	Total Attempts	Warning
TikTok	35	0	35	0
Instagram	35	0	35	1
Twitter	21	46 (69%)	67	0
Facebook	34	4(10%)	38	1
Mastodon	35	0	35	1

Limitation and Future Work

Limitation

- Number of Applications & experiment duration
- Limited visibility

Future Works

- Scale the experiment
- Periodically checking previously posted links
  - Long term effect
- Usability survey

Conclusion

- Alarming state of malicious URL sharing in OSN
- Role of URL Blocklisting services
- Observed a lack of usable security

Thank you for your attention!

Muhammad Hassan
PhD Student, School of Information Sciences
University of Illinois at Urbana-Champaign
✉ *mhassa42@illinois.edu*