**Introduction**

Phishing attacks on social media are recently increasing. Social media is a big target for hackers because people post personal information on their social media accounts. Some people post their information about their families and daily activities on social media. Attackers use phishing attacks to gain some personal information so that they steal identity or sell that personal information. There are studies about phishing attacks on Social media. However, there aren’t enough studies just yet. Attackers send a friend request or connection request on social media. When users accept the invitation, it is easier for attackers to send a malicious link as a direct message and lure users to malicious websites or download malware.

For this research, I focused on Instagram. According to “Online social networks security and privacy: comprehensive review and analysis**”,** Instagram has a billion users.

**Problem domain**

The problem domain I am explaining here is phishing attacks on social media. I especially focused on Instagram. Attackers send requests to connect if the account is public and then send malicious links through direct messages. Then they can steal personal information to sell or for identity theft. Attackers also learn more about a person by following and looking at the posts.

**Hypothesis**

My hypothesis using privacy settings on social media can reduce the chance of phishing attacks. If users make their accounts private and if they do not accept invitations from strangers, they can mostly protect themselves from phishing attacks.

**Empirical data**

For this paper, I used two fake Instagram accounts and one real account. I tested by playing around with the privacy settings and sending messages between the accounts. The empirical data I presented is qualitative and not quantitative. Since quantitative data takes more time and resources and can not be done by testing only two accounts.

|  |  |  |
| --- | --- | --- |
|  | **Public account**  **Direct message enabled** | **Private account**  **And direct message disabled** |
| Can send message and link if send is not a follower | Yes if message is enabled | No if message is disabled. Yes if message is on |
| Can send message and link if sender is a follower | yes | No if message is disabled. No If message is turned on. |

**Findings**

I created two Instagram accounts. Then I used my son’s real Instagram account. I asked my son to make his account public temporarily. I was able to send him a message even if I wasn’t part of his followers. Then I made my first fake account private and I send a message from my second fake account. I was able to receive the message even if my account was private. Then I turned off direct message on my first account and tried to send a message from my second account but that didn’t go through. What I learned from my Instagram research is that, setting accounts to private still attackers to send a direct message to targets. Turning off messages helps prevent getting direct messages. However, this will also prevent friends or followers to send direct messages. Setting an account to private doesn’t prevent direct messaging but it helps prevent attackers from following a target user and learning more information about the person. Unless the person accepts invitations from random people, people who are not followers can’t see the person’s post.

From my findings, I believe that Instagram users should make their account private at least and if it is possible, turn off direct messaging to not get malicious links from attackers.

**Related research**

<https://link.springer.com/article/10.1007/s40747-021-00409-7>

<https://www.mdpi.com/1999-5903/10/12/114/htm#B13-futureinternet-10-00114>