The Impact of using Mobile Phones on Privacy of Students in the Kingdom of Saudi Arabia

Alanood Alenizi† and Esam Khan††

†Computer Engineering Department ,Umm Al-Qura University, Makkah, Saudi Arabia.
††The custodian of the two Holy Mosques institute of Hajj & Omrah research, Umm Al-Qura University, Makkah, Saudi Arabia

Abstract

In this study, we aimed at exploring the current practices of using mobile phones by students in Saudi Arabia and identifying the potential data privacy risks that they are exposed to. The key findings from the study was that although a majority of students are aware of data privacy, many of the respondents were willing to chat with unknown people online and a considerable number of those participants opened URLs sent from strangers. This is a huge data privacy risk since it may result in the disclosure of their personal information without the knowledge that the websites were deceptive sites that posed a threat to their personal data, which led to several risks to their personal data, such as theft of personal accounts, identity cards, information, and personal photos. Based on the finding and due to the lack of research and commercial efforts of detecting malicious URLs on mobile devices, we developed a system, Suspicious URL Detector, which is targeted to support mobile users to seamlessly verify URLs before they can be opened. Our system is composed of a mobile app and a URL verification server that is backed by PhishTank [1], a user-contributed blacklist of suspicious URLs. The mobile app is also designed to be user-friendly and lightweight to ensure it performs well on mobile devices with limited resources.

Key words:

personal data privacy breach, suspicious URLs, blacklisting, phishing, Phish tank.

1. Introduction

Smartphones form an integral part of people's everyday lives, including those of students, no matter what their genders or backgrounds. However, despite the undeniable benefits of smartphones, they can also pose serious threats to user privacy due to the huge amount of personal data that they store. Privacy has become a big challenge facing smartphone users. In fact, it is impossible to guarantee 100% privacy of personal information, especially when using social networks, since personal information can be misused by users [2]. in addition, Smartphones, with its huge benefits of facilitating easy communication and entertainment, have form an integral part in modern society. However, that also makes smartphone users vulnerable to cyber-attacks in general and data phishing.

In recent years, the number of phishing attacks has increased significantly, according to trend reports by [3]. The number of unique phishing sites was reported at over 48,000 in January 2019 and then shot up to over 81,000 in March 2019. Therefore, it is important to provide a system that helps protect users' data on mobile devices from phishing. There have been a considerable number of efforts from both academia and industry to address and mitigate this issue. However, most of them have been targeting desktop and web environments while mobile platform URL verification has been largely neglected. Blacklisting is one of the common techniques in the field. It is based on the idea of collecting a blacklist of malicious URLs from different sources and using such a blacklist to validate against a new URL [4]. From the machine learning paradigm, a lot of effort has been made to build classification models [5] based on SVM technique and use such models to verify new URLs. In order to develop classification models, URL data have to be collected and transformed into features. A URL being verified at runtime has to also be transformed to feature in order for the models to interpret. Such a process typically would require a huge amount of effort every new model needs to be trained and considerable memory consumption to turn URLs to features at runtime. While this is less as an issue on desktops and webs, it raises a concern on mobile since smartphones and tablets are at much lower memory and processing powers compared to desktops and laptops. In this paper, we propose a new system that allows URLs to be verified as to whether they are safe to browse or suspicious on mobile devices. Specifically, we built an Android mobile app and a URL verification server which is backed by PhishTank [1], a user-contributed blacklist of suspicious URLs around the world. Such a setting helps us avoid the burden of self-maintaining the URL blacklist while ensuring its high quality. The mobile app is also

Manuscript received September 5, 2020
Manuscript revised September 20, 2020

DOI: 10.22937/IJCSNS.2020.20.09.18

designed to be user-friendly and lightweight to ensure it performs well on mobile devices with limited resources.

The rest of the paper is presented as follows. In the next section the related literature is reviewed. Third section presents the research methodology and the following section presents the research results. The fifth section presents discussion of the survey and Based on that; we present our approach of building the mobile application for malicious URL detection. We conclude with analysis the results. The last section contains the conclusion and future work.

2. Related work

In this section, we discuss the background and related research of this work. We start with provide a general background of data privacy and the common issues related to privacy breaches such as phishing. We also discuss range of existing research and commercial effort on detecting malicious URLs.

2.1 Data privacy

According to [6], privacy means reaching a specific thing. [7] claimed that privacy is a set of policies and conditions that requires a system to protect users. [8] defined privacy as the protection of personal data from being maliciously used by only allowing certain entities to access personal information by making it visible to them. Moreover, [9] indicated that privacy is more important in applications that want to store location information to prevent it from being shared with others.

2.2 Common Uses of Mobile Phones

[10] investigated the differences between men and women in their use of their mobile phones. The authors found that women generally use their devices for calls, taking photos, listening to music, and sending and receiving messages more than men. On the other hand, social networks and Internet browsing are more popular in the men group. These results were consistent with the results of [11], which claimed that men use their phones for business purposes, while women use them for social media and keeping contact with others.

[12]found that in Europe, women tend to use text messages for communication more than their men counterparts. That is also consistent with the findings from [13]. However, [14] found that in Pakistan, men use their phones for calls and text messages more than women. That was due to the cultural aspect of the country, the research claimed.

2.3 User Awareness of Data Privacy

Privacy is one of the most troubling issues for service providers and users. Privacy has made some people fear for their personal information, while others have become reluctant to use the Internet in general [15].

In a study of 4,000 students from Carnegie University,[16] found that a large proportion of students who use social networks were not aware of privacy risks to their personal information and thus were vulnerable to third party misuses of their information.

[17] reported a consistent outcome that younger users on social networks and online environments were not keen about the privacy of personal information compared to older users who have shown interest and concern about the issue of privacy. Most younger users share their information without knowledge about the risks concerning the misuse of these data.

[16] conducted a survey to understand Facebook users' concern regarding data privacy. They found that 91% of users uploaded their photos, 51% shared their current locations and 40% revealed their private phone numbers. The authors claimed that the more information is shared, the more risks the users were exposed to since such information can be exploited by hackers or malicious users.[18] claimed that women believe Facebook is a trustworthy social network for sharing their photos while in reality data privacy could be leaked on any platforms.

2.4 Phishing

Phishing is a common way to steal a user's personal information by using suspicious URLs that pretend to be associated with legitimate sites [19]. Common examples of phishing attacks involve mimicking the online communications of banking services. Recently, experimental research has shown phishing attacks to be alarmingly effective and dangerous.[20] Risks to personal information on social networks take many forms. For example, these risks can be caused by hackers who access personal data using phishing attacks with suspicious URLs. Identity theft is one of the most risks that users face [20] Also, if a blackmailer gains access to a user's sensitive data, it may lead to physical or sexual extortion and financial risks [20]. Phishing can be performed across various means, including emails, social networks, messages, and even phone calls. A standard phishing technique used by hackers is to create the illusion that they are trustworthy by falsely claiming their websites or email addresses belong to highly trusted organizations or governments. In many instances, phishing websites or emails are designed to exactly mimic the original content to confuse users [20]. [21], from their survey, reported that more than 90% of respondents were deceived by the best phishing site. 23% participants observed the contents of the website without looking at the remaining parts, for example, address bar, status bar, or any other security bars. Statistics of phishing attacks reports have pointed out that some phishing websites persuade users to provide sensitive information to attackers. In addition, two million users disclosed information to phishing websites resulting in about 1.2 billion for US banks. Also, reported about 2780 phishing websites in March 2005. This type of attack requires initial information about the victim in order to infiltrate the victim's personal accounts through a trusted site or another person in the hope that the victim believes that the site is legitimate, then the victim discloses their username, password, credit card number, or other identification information [22].

2.5 Existing Attempts to Detect Suspicious URLs

Malicious URLs are the cornerstones of Internet criminal activities. Generally, there are two key approaches to addressing this issue: machine learning based and non-machine learning based techniques.

2.5.1 Non-machine learning based approaches

The key idea of this approach is to collect a number of suspicious URLs and keep them up to date. This collection of URLs would serve as the source of truth to determine if a certain URL is clean or malicious. Blacklists have a huge advantage that they are generally quick and simple to get started.

2.5.2. Machine learning based approaches

While these techniques create a very promising paradigm, most of them rely on a high number of features, which means the training data has to be very huge and thus very time consuming to build and train. Moreover, the techniques relying on features like WHOIS, DNS (e.g., [5] is not so practical since at runtime the details of the URL being checked have to be obtained from a server. Moreover, the URL has to be converted to those features in order for the classification model to work. That process would likely increase the check execution time especially on mobile devices.

2.6 Commercial Solutions

Most of the discussed related work focuses on web platforms. Malicious URL detection has been largely neglected on mobile platforms. According to our review on both Android Google Play Store and Apple App Store, there are only a few applications which are focused on addressing the issues. In the rest of this section, we provide an overview on how these applications work and their limitations.

2.6.1 Safe Search Browser - Secure + Parental Control

This app's primary purpose is to provide a safe web browser for users to search and browse the Internet without any privacy concern. It blocks the websites from accessing information on the user devices. Moreover, it would help filter out malicious URLs from the search results. However, since the app is not developed to detect malicious URLs as a main goal, it does not help if a user attempts to open a URL outside the app (for instance, tapping on links sent in WhatsApp or emails)[23].

2.6.2 Anti-Phishing Awareness

This mobile app is primarily concerned about educating users on what phishing is and how to avoid it. It allows users to take lessons such as what is domain name or ip address. Users can also take quizzes to validate their understanding. The app also provides a "scanner" which takes a URL as input and verifies if such a URL is safe or malicious.

Since it is not a primary focus of the app to verify URLs (it is rather focused on the education of phishing. Moreover, users have to enter URLS manually to verify with the app as it does not automatically invoke the check when a user taps on a URL. That would limit its applicability in reality [24].

3. METHODOLOGY

3.1 Respondents of the study

This study was based on the use of a probabilistic sampling method. Consequently, the study sample was selected from the female and male students of three universities in Saudi Arabia (King Saud University, Umm Al-Qura University and King Abdul-Aziz University). Our sample also included students from three high schools, in order to provide a comparison between different age groups. The criteria for selecting surveyed were that they own a mobile phone and have at least one social network account.

3.2 Survey Results:

3.2.1. Participants Demographic

Out of the 447 respondents who completed the survey, 199 (45 %) are male and 248 (55%) are female. Fig. 1.1a illustrates the summary of our participants demographic with respect to gender and education level while Fig. 1.1b provides a summary from gender/age perspective. As can be seen, most of our respondents were bachelor students, followed by high school students. Moreover, most participants were in the age group of 19-27

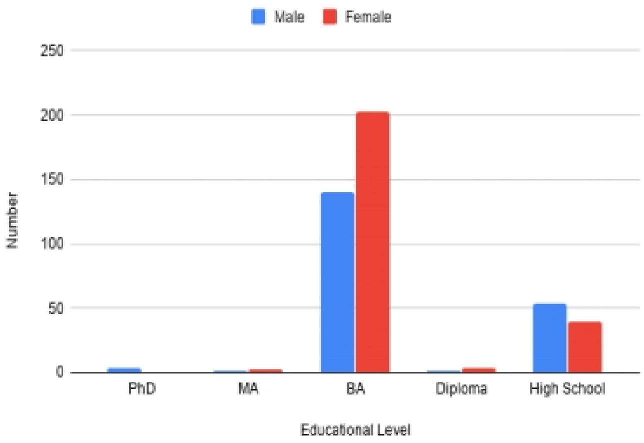


Fig. 1-a Participants demographic by gender and education

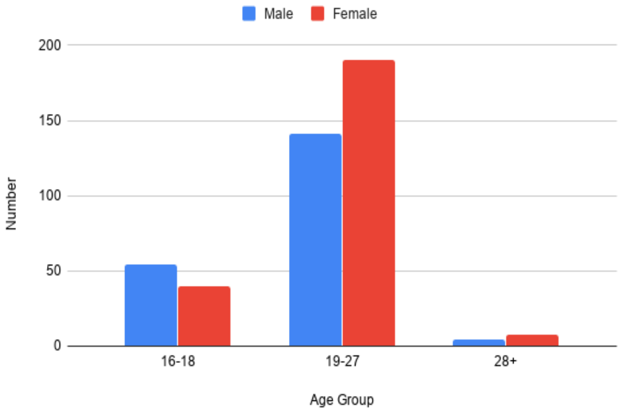


Fig. 1-b Participants demographic by and education and gender /age

3.2.2. Usage of Mobile Phones

In this part of the survey, participants were asked about their common use cases of mobile devices and their preferences regarding social networks.

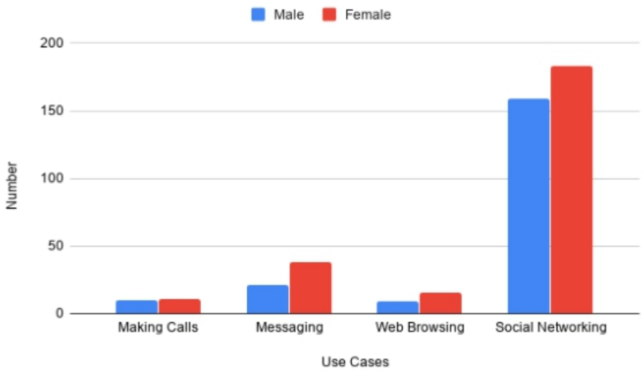


Fig. 2 Common use cases of mobile phones

According to Fig. 2, social networks are where the participants spend most time, which was indicated by 72% female respondents and 80% male respondents. Messaging is the second most popular usage, while call and web browsing come next in the list. These results further confirm the increasing popularity of social networking platforms, such as Facebook or Twitter, in comparison to traditional mobile phone usages, such as calling or messaging.

3.2.3. Data Privacy Awareness and Practices

Another primary concern in the survey is the current state of students' level of awareness regarding data privacy and their practices of privacy protection while using smartphones. In this section, we first present the key results in this part of the survey. We then discuss our conclusion from such results.

3.2.4. Data Privacy Concern

Fig. 3 presents the responses from participants regarding whether they are concerned about their data privacy while using smartphones (data are in numbers of responses). As can be seen, it is consistent between male and female responses in each age group. In fact, higher education students showed a high level of concern regarding data privacy with most responses being either "Strongly Agree" or "Sometimes Agree". In the high school students' group, only about half of the respondents across both gender groups agreed that they have concern about data privacy.

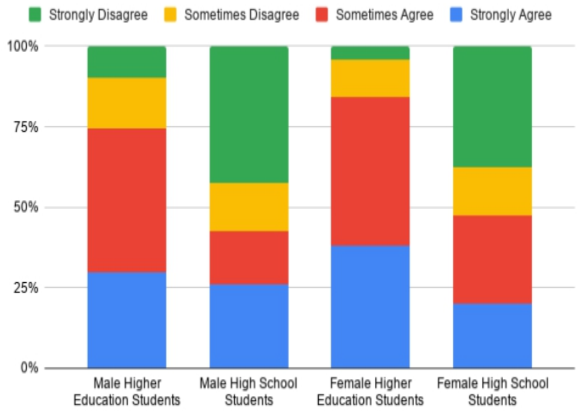


Fig. 3 Responses regarding concern about data privacy when using mobile phones

Interestingly, despite the expressing the general concern regarding data privacy, out results found that the respondents are less concerned when being asked for sharing personal information when using smartphones (e.g., on social networks). In fact, Fig. 4 shows while more than 50% of participants in the higher education groups showed the concern regarding sharing personal information, the number of "Strongly Disagree" responses were relatively high. In the high school group, the responses from male and female participants are interestingly opposite to each other. While male students are generally not worried about sharing personal information, most female students indicated that they are.

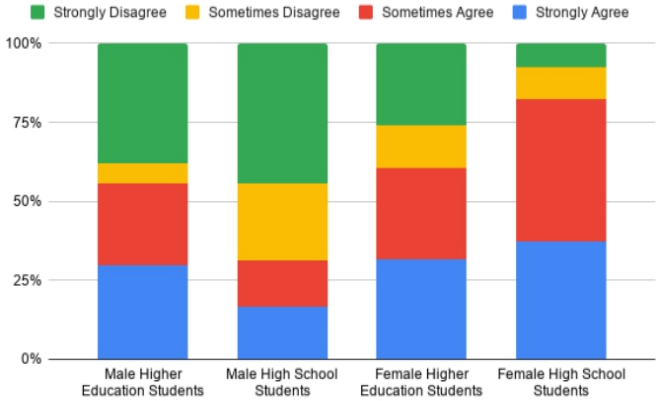


Fig. 4 Responses regarding concern about sharing personal information when using mobile phones

In the next part of this section, we explore the results on how the participants use the common tools for data privacy protection while using smartphones.

3.2.5. Social Network Privacy Settings and Policies

In this part of the survey, we targeted to understand the use of privacy settings and policies by students. Fig. 5 indicates that for all gender/educational level groups, over 50% of students rarely or never read data privacy terms and conditions when they registered on social networking platforms. While the patterns are very similar between higher education and high school male students (about 25% indicated they never read terms and conditions and about another 25% indicated they always do), there was a different in terms of privacy awareness found among female students. Specifically, while there are only 5% of female high school participants said they always read terms and conditions and about 55% of them revealed that they never do that, the respective numbers for higher education female respondents were about 22% and 25%. This implies that female students are generally more concerned about privacy while they get older.

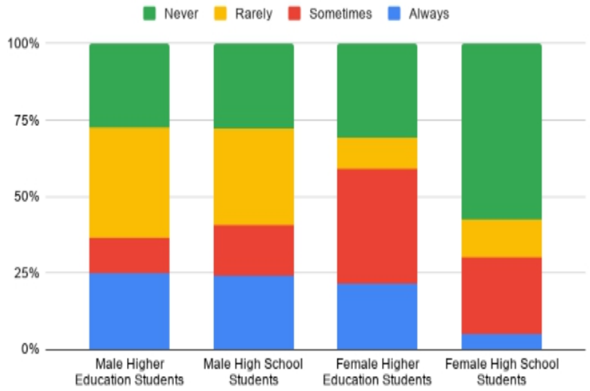


Fig. 5 Responses regarding whether students read privacy terms and conditions

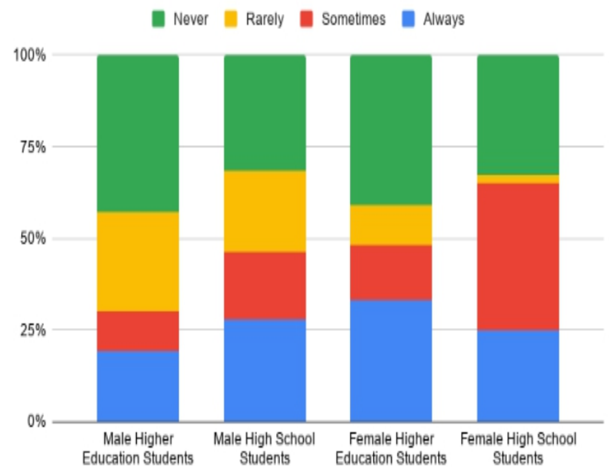


Fig. 6 Responses regarding whether students change the default privacy settings

Participants were also asked about whether they changed the default privacy settings of their social media accounts. It was found that most respondents use the standard default privacy settings in their mobile applications (indicated in Fig. 6. Generally, default privacy settings imply the average security level. Thus, they can be both beneficial and harmful at the same time. In some situations, these settings may allow the sharing of personal information without the users' knowledge. This finding is in line with another of our findings that a majority of students in the survey were not familiar with privacy settings on social network platforms.

3.2.6. Use of Locks

In this part of the survey, we aimed to explore the use of locks, which is one of the most basic security measures on smartphones. Promisingly, we found that most participants had safety locks on their mobile phones enabled. Fig. 7 depicts that about 87% of male high school students and 96% of higher education students responded "Yes" to the question as to whether they used safety locks. For female students, the numbers were 88.1% and 94.4%, respectively.

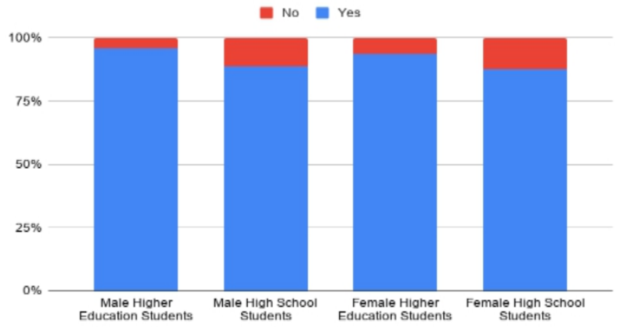


Fig. 7 Responses regarding whether students use locks on their mobile phones

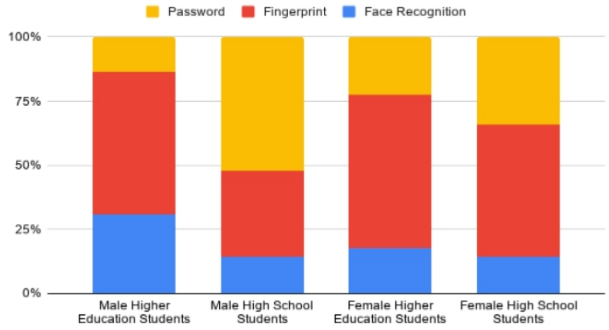


Fig. 8 Responses regarding preferred types of locks

Fig. 8 shows the types of mobile phone locks used by the participants. Fingerprint recognition is the most common practice among the participants except for the male higher education students in which nearly 50% of the respondents used a password lock while the number of fingerprint recognition users represented only about 30%. It is a general consensus that biometric-based locks, such as fingerprint recognition, is not only a quick way of unlocking a mobile device, but also provides a more secure option over password-based alternatives. That is because the biometric details of the owner of the device are required to unlock it and thus it is much harder to hack into compared to passwords.

3.2.7. Use of Public Wi-Fi

Fig. 9 presents the responses of the participants regarding whether they connect their mobile phones to open Wi-Fi networks in public places. More than 75% of male high school students and more than 55% of male higher education students answered "Never" and "Rarely" to the question. For female students, about 55% of higher education students and 33% of high school students answered "Always" and "Sometimes." In most cases students do not need to connect to public Wi-Fi since their devices are already connected to private 3G or 4G networks. However, since the number of students who still regularly connect to public networks (answered “sometimes” or “always”), there are still data privacy risks to those students.

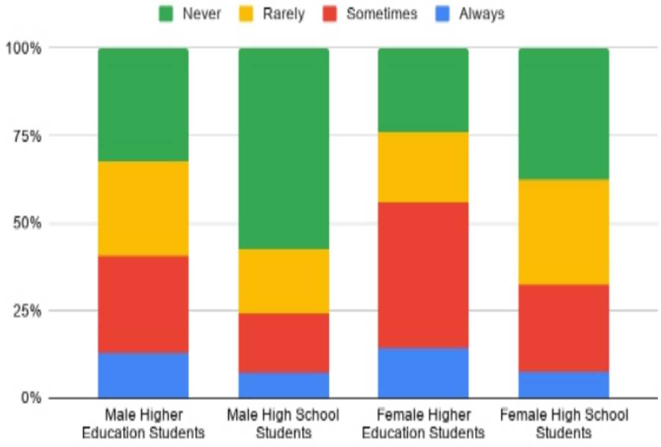


Fig. 9 Responses regarding whether students use public Wi-Fi

3.2.8. Contact with Unknown People on Social Networks

In this part of the survey, we aimed to explore the use of social networking by students. Particularly, we focused on identifying whether they are willing to be in contacts and strangers and opening links from them since that is one of the key common method of phishing.

Fig. 10 shows that a high proportion of the participants were willing to chat to strangers online. In fact, 80% of male high school students and 50% of higher education students were happy to have a conversation with an unknown person online. The results from the female respondents were much lower, with only 38% of high school students and 36% of higher education students providing the same answer. We also found that nearly 70% of male high school students and 35% of higher education students did open URLs from strangers before at least once Fig. 11, Without checking the main source of these URLs. The numbers from female respondents were much lower, with only about 50% and 15%, respectively. Most respondents in the survey also showed that they were unclear about the effect of opening a URL on their mobile devices.

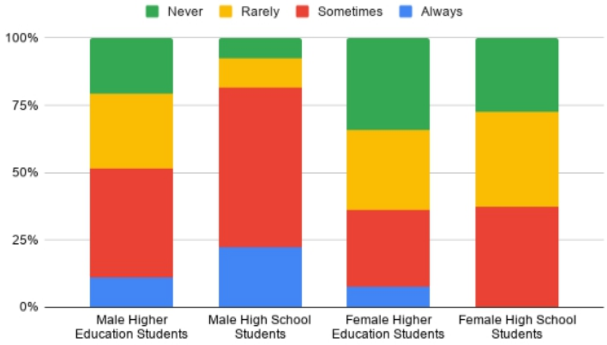


Fig. 10 Responses regarding whether the participants chat with unknown people on social networks

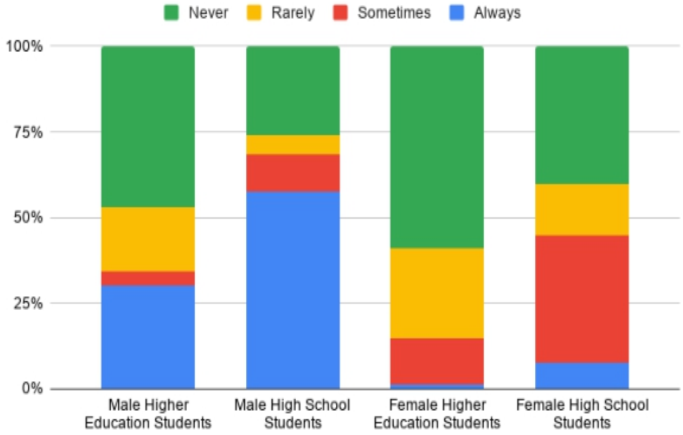


Fig. 11 Responses regarding whether the participants are willing to open links from unknown people

3.2.9. Sharing mobile phones

In this part of the survey, we target to understand if it is common that students share their mobile phones with others for any reason. Fig. 12 indicates that 75.8% of male higher education students answered “Never” and 14.4% answered “Rarely.” Adversely, we found 60% of male high school students share their phones with their family and friends. For female students, 55% of the higher education students answered “Never” and rarely sharing their phones. 57% of high school students answered sharing their phones.

An important notice from the results is that, phone sharing is less common when students get older, which is reflected by 75% of higher education male students and 45% higher education female students who claimed they never shared their mobile phones with anyone, compared to the numbers from high school students of 27% and 26%, respectively.

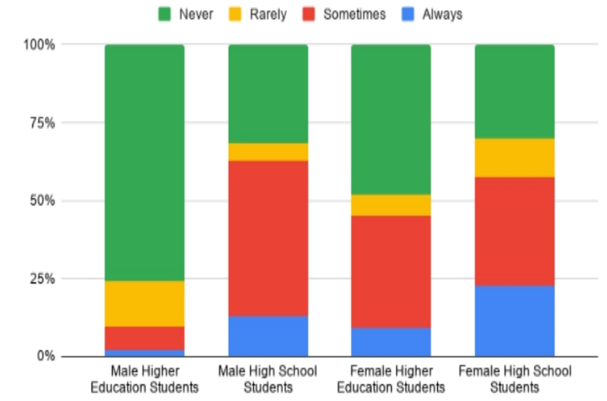


Fig. 12 Responses regarding whether the participants share their mobile phones with others

The survey results also show that most respondents were cautious about sharing their mobile devices with someone else. Fig. 13 presents the key reasons why the students felt that devices should not be shared. In fact, there was a strong consensus among the groups that privacy and exposure of personal information are the top reasons for not sharing devices. Specifically, 45% of male high school students and 35% of higher education students picked privacy as the key reason, while about 60% of female high school students and 40% of higher education students gave the same answer. The likelihood of exposing personal information was selected by 25% of male high school students and 40% of higher education students. For female participants, about 20% of both high school and higher education students chose likelihood of exposing personal information as their answer.

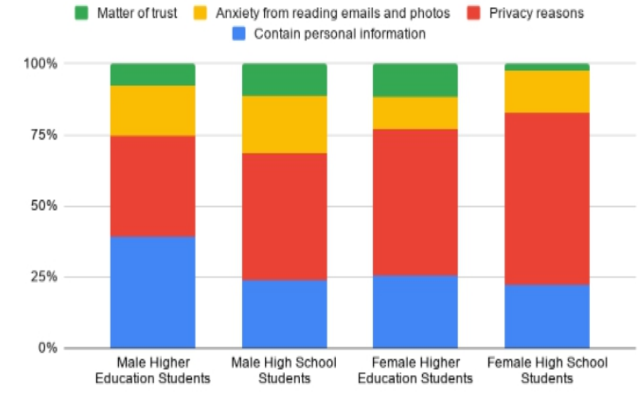


Fig. 13 Responses regarding why the participants think mobile phones should not be shared

3.3 Experience with Data Privacy Issues

In this section, we discuss the findings regarding the data privacy issues that the participants have experienced themselves and what the impacts of that on them.

In the survey, the participants were also asked if they have experienced personal data loss when they opened suspicious URLs or downloaded applications from suspicious URLs. Fig. 14 shows about 11% of higher education male students and 9% of high school male students have experienced hack into their personal accounts in social networks, while female students reported about 8% and 15%, respectively. Regarding the theft of identity information, 9% of male higher education students and 6% of male high school students have experienced this issue, while fewer female respondents experienced the same issue, reporting at 4% and 5%, respectively. In regard to theft of personal photos, about 8% of male higher education students and 4% of high school students have been victims, while 9% of female higher education and 7% of high school students have experienced the same problem.

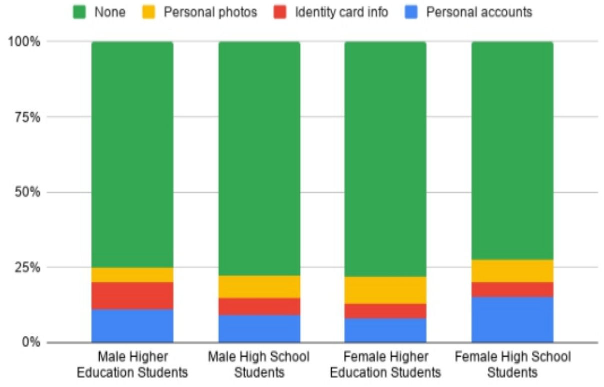


Fig. 14 Responses regarding what data loss issues the participants have encountered

4. Discussion

In this study, we have found that most students participating in the survey are aware of data privacy to some extent. A majority of them do not share mobile phones with others for privacy and security reasons. We also found that most of them use locks on their devices to prevent unauthorized access and fingerprint being the preferred choice by many of them. However, while social networking is their primary activity on mobile phones, a majority of students do not pay sufficient to privacy settings and end up with using the default settings in most cases. In addition, we also found that many of the respondents were willing to chat with unknown people online and a considerable number of those participants opened URLs sent from strangers. This is a huge data privacy risk since it may result in the disclosure of their personal information without the knowledge that the websites were deceptive sites that posed a threat to their personal data, which led to several risks to their personal data, such as theft of personal accounts, identity cards, information, and personal photos.

Despite being a threat, communicating, making friends, and exchanging URLs are common activities of Internet users. Thus, it is not practical to prohibit such behaviours on the Internet despite that it carries risks. A mitigation approach is therefore detecting phishing attempts through malicious URLs. This was the motivation for the researcher to build an application that seeks to detect phishing attempts (suspicious URLs) to reduce penetration cases.

5. Our Approach

With the objective of providing a performant and convenient method for helping mobile users detecting malicious URLs, we decided to build a mobile application which is backed by Phishtank, a user-contributed blacklist of suspicious URLs around the world. This approach provides a number of key benefits:

- Blacklist provides a lightweight approach where the main processing is done by backend, making it very quickly to be executed on the app.
- Being a lightweight approach means less memory and energy consumption which are limited on mobile devices in comparison with web applications which run on laptops or desktops.
- Phishtank is a popular user-contributed platform where the blacklist of malicious URLs is contributed by a large number of contributors around the world (contributions are reviewed to avoid false positives). This keeps the url collection up to date on a regular basis.

5.1 Implementation Details

The following diagram illustrates the architecture of our system. Basically, there are two main components that work together: the *SuspiciousUrlDetector* app that captures the URLs to be checked, and the *SuspiciousUrlDetector* server that handles the URL queries from the app and collects blacklist updates from *PhishTank* Fig. 15

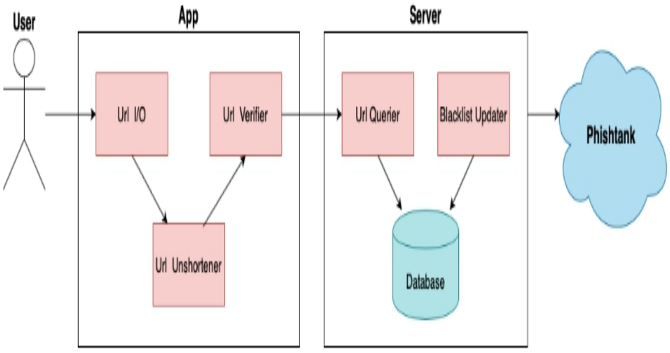


Fig. 15 The suspicious URLs detection system's high -level architecture

5.1.1 SuspiciousUrlDetector Mobile App

In this section, we describe the key elements of the mobile app and their roles.

URL I/O

This component is responsible for taking URL input from users. There are two forms in which URLs are provided to the app:

1. By manual user input: when a user opens the app and enters the URL into the app. The “URL I/O” component provides the user interface for URLs to be keyed in.
2. By automatically detecting that a user has tapped on a URL in a certain app on the device and requesting the user to verify that URL in the app. Once the user accepts to check the URL with the SuspiciousUrlDetector app, the URL I/O component proceeds to the next step in the detection process using this URL.

This component also supports URL format validation (in case a URL is supplied in the wrong format and gets results from the detection and displays it to users).

URL Unshortener

URL shortening is a common technique used to create a shorter URL to be more user friendly and easier to type. There are a number of websites that provide shortening services. Some of the popular ones are bit.ly and rebrandly. Using such a service, a long website address, such as https://www.morningstar.com/insights/2019/06 /18/great-advice, could be shortened to only https://rb.gy/i8kxzd.

Such a shortening technique could be simply used by hackers to bypass blacklist-based URL verification systems. Therefore, in our work, we developed a URL unshortener to uncover the original URLs hidden behind short URLs. Our URL unshortener is based on unshorten.me–an API that unshortens URLs that have been shortened by various services, including goo.gl (Google), fb.me (Facebook), t.co (Twitter), bit.ly,Tiny URL, ow.ly, and others. In our system, the URL unshortener would receive a URL passed from the URL I/O and attempt to perform the unshortening process on the URL. In the case the URL is standard (not shortened), the same URL would be returned as output. If the URL ends up being unshortened, the result would be output to the next stage in the URL detection process.

URL Verifier

As its name suggests, this component is responsible for answering the question as to whether the URL is malicious. It mainly queries the SuspiciousUrlDetector server to obtain the results.

5.1.2 SuspiciousUrlDetector Server

This component handles the important job of periodically retrieving the blacklist updates from PhishTank and responding to URL queries from the app. It has two main elements, discussed as follows.

Blacklist Updater

We decided to build the blacklist on our server to periodically fetch updates from PhishTank and store it in the database stored on the same server. Doing this helps to achieve a number of benefits:

1. The mobile app does not need to do the heavy lifting job of fetching and storing PhishTank data since it is very large and would thus consume considerable bandwidth and energy. Performing and keeping PhishTank data on the server guarantees the mobile app to be lightweight, as per our research objective.

2. Storing PhishTank data on our own server gives us full control of the data and avoids the dependency on PhishTank for individual URL verification. Our system would thus still allow URLs to be verified even if PhishTank was not available for a certain period.

URL Querier

URL querier receives query requests from the URL verifier in the mobile app, then checks with the database that stores PhishTank data and responses with the result of the verification.

5.2 User Flows

In this section, we provide some demos of what the user flows in the app look like.

5.2.1 Flow 1: Users manually enter URLs

As depicted in Fig. 16 this flow starts with a screen in which users can enter a URL to be verified Fig. 16.a. If the verification turns out to be good, the message is displayed Fig 16.b. Otherwise an error message is shown to the user to warn them that the URL may be malicious Fig. 16.c

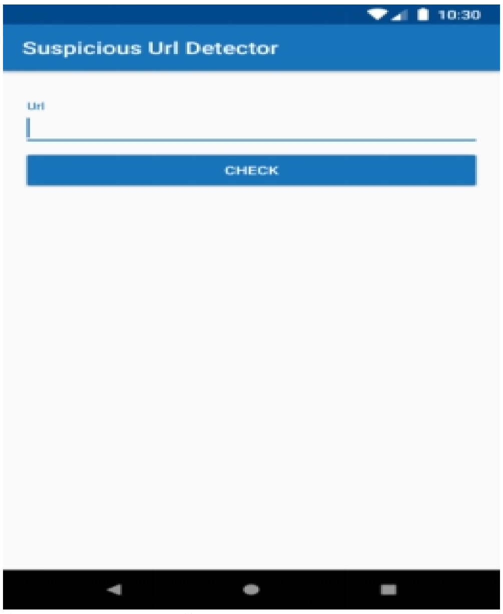
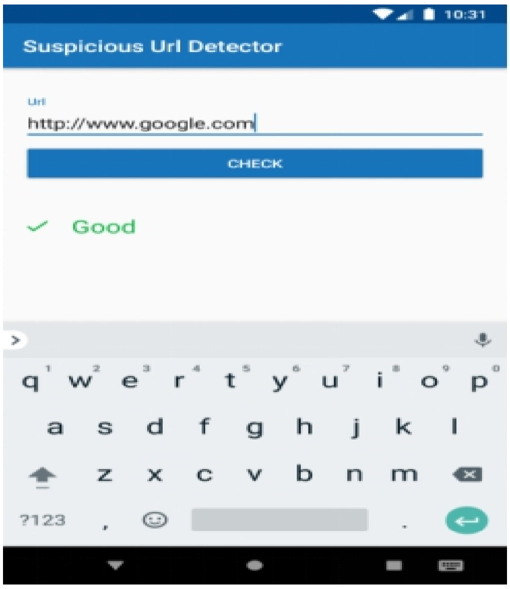


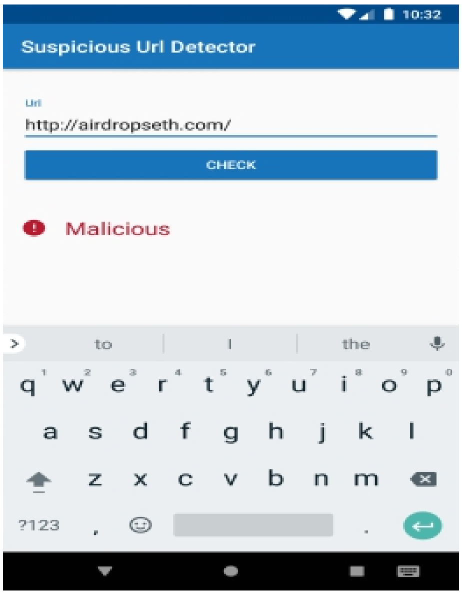
Fig. 16.a Users manually enter URLs



http://www.google.com

✓ Good

Fig. 16.b The message displayed if a URL is good



Url

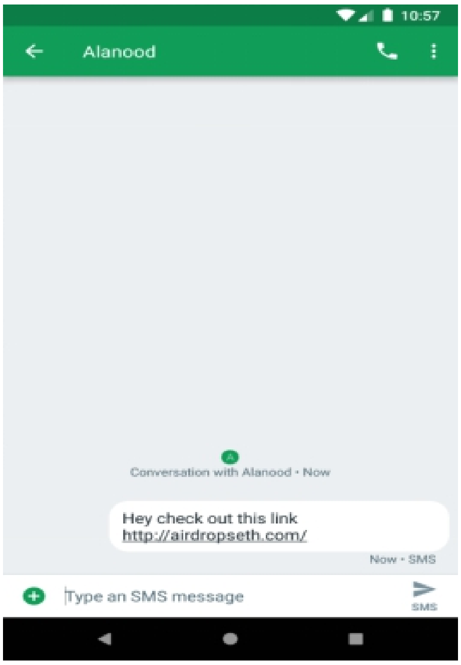
http://airdropseth.com/

Malicious

Fig. 16 .c The message displayed if a URL is Suspicious

5.2.2 Flow 2: Users open URLs from another mobile app

Fig. 17 describes this flow. Suppose a user taps on a URL from an application, such as a messaging app , Fig. 17.a the SuspiciousUrlDetector app would be able to detect that interaction and request the user to launch the app to verify the URL Fig. 17.b. Once the user accepts the request, the app would start querying the Server about the URL and display the result back to the user Fig, 17.c.



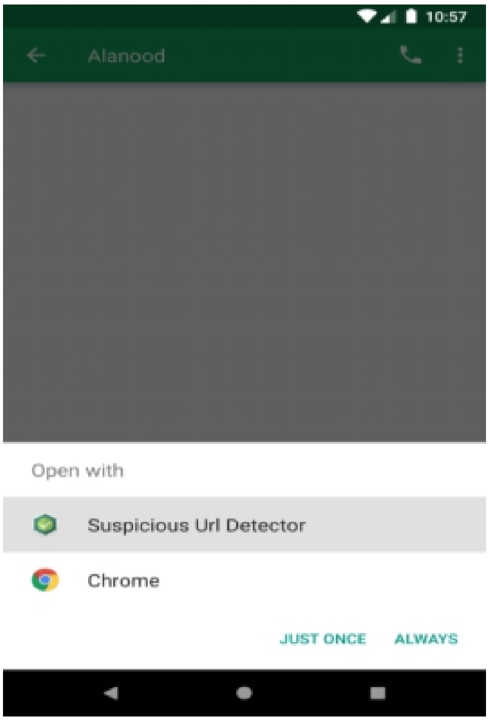
Conversation with Alanood • Now

Hey check out this link
http://airdropseth.com/

Now • SMS

Type an SMS message

Fig. 17.a Users open URLs from another mobile app

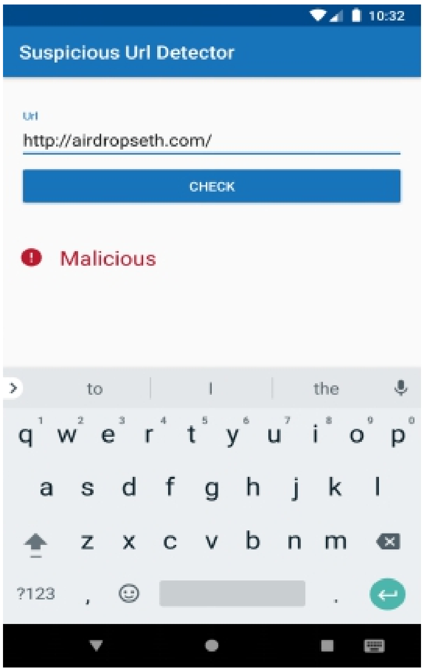


Open with

Suspicious Url Detector

Chrome

Fig. 17.b The app request the user to launch the app .



Suspicious Url Detector

Url

http://airdropseth.com/

Malicious

Fig.17.c The message displayed if a URL is Suspicious

6. Evaluation

6.1. Correctness Evaluation

In order to verify the correctness of our system, we used Google's Transparency Report, a free service provided by Google to help verify if URLs are suspicious or legitimate, as the source of truth. That means we assume that Google's Transparency Report is always correct and that our system would be considered incorrect whenever its result is inconsistent with that of Google's Transparency Report. We also involved 2 commercial mobile apps that performs similar detection (Safe Search Browser - Secure + Parental Control and Anti-Phishing Awareness) in this test to compare the correctness of Suspicious URL Detector with them.

6.1.1. Experiment Setup

To perform the experiment, we randomly selected 100 URLs and checked them one by one in each of the platforms (Suspicious URL Detector, Google's Transparency Report, Safe Search Browser, and Anti-Phishing Awareness). We then collected and analyzed the results.

The analysis of the results was driven by *precision*, *f-measure*, and *recall* [25]. Precision is the ratio of correct positive predictions out of all positive predictions produced. Recall is calculated by dividing the number of true positives by the total number of true positives and false negatives. F-measure is used to combine both precision and recall into one measure which captures both properties. Like precision and recall, a score of 0.0 presents a poor F-Measure, while a best or perfect F-Measure score is 1.0. The three measures are calculated according to the following formulas:

$$precision = \frac{TP}{TP+FP} \tag{1}$$

$$recall = \frac{TP}{TP+FN} \tag{2}$$

$$F-measure = \frac{2 \times precision \times recall}{precision + recall} \tag{3}$$

where TP means True Positive, FP means False Positive, and FN means False Negative.

For all three measurements, the closer they are to 1 the more accurate the result is.

6.1.2. Experiment Results

Table 1 summarizes our results. The numbers collected are based on using Google's Transparency Report as the benchmark. For instance, if the URL is deemed suspicious by Google's Transparency Report and is also considered suspicious by the app being tested, it is considered a "true positive." However, if the app indicates that such a URL is valid, it is then considered a "false negative."

	Suspicious URL Detector	Safe Search Browser	Anti-Phishing Awareness
True Positive	68	62	67
True Negative	30	30	30
False Positive	2	3	1
False Negative	0	5	2
Precision	0.97	0.95	0.98
Recall	1	0.92	0.97
F-measure	0.98	0.93	0.97

Table 1: Correctness evaluation results

According to the results, our system's performance was very close to that of Google's Transparency Report (all the measurements were very close to 1). It also shows that our system outperformed the Safe Search Browser app in the test (0.97 vs. 0.95 precision, 1 vs. 0.92 recall, and 0.98 vs. 0.93 f-measure).

6.2. Usability Evaluation

To evaluate the usability of our system, we organized a user study in which we recruited 15 participants from a variety of backgrounds to use the Suspicious Url Detector app to perform a number of predefined tasks (scenarios) and collected responses from them on how they completed the tasks. In the following, we describe the experiment setup and its results.

The Tasks

The tasks in this experiment were defined based on the two key user flows described in Chapter 4. The first user flow involves manually entering a URL directly into the Suspicious URL Detector app and verifying it. The second user flow involves tapping on a URL from another app and invoking the Suspicious URL Detector app to verify it. To analyze users' performance, we collected the number of taps (clicks) they needed to verify the URLs and the time they took to complete each task. Our data show that all participants successfully completed both tasks with correct results. They also only needed to make a maximum of 2 taps (90% of them only needed one tap, which is the optimized situation) to complete each task. Fig. 18.a and 18.b show the time taken by each participant to perform Task 1 and 2, respectively.

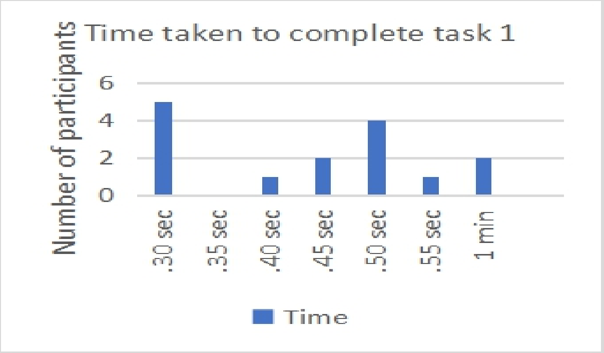


Fig. 18.a Time taken to complete task 1

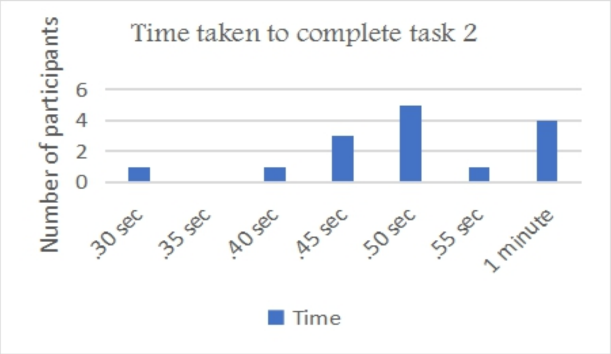


Fig. 18.b Time taken to complete task2

As shown in the data, all participants only needed one minute or less to complete each task the first time they used the app. For Task 1, the majority of users only needed to take 30 seconds, while on Task 2, the majority of users needed about 50 seconds.

Post-experiment questionnaire

We asked participants a number of questions after they completed the tasks to get a better understanding about how they felt about the usefulness and functionality of the app. Each question was in the form of a rating from 0 to 10 in which 0 means "extremely hard to use/useless" and 10 means "extremely easy to use/useful." Fig. 19.a and fig, 19.b show that most users believed the app to be easy to use and useful for protecting users from phishing.

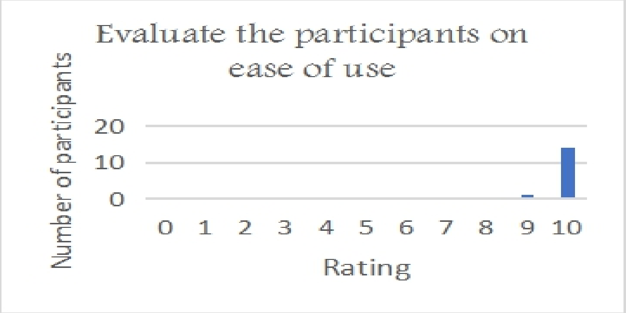


Fig. 19.a Participants evaluation on ease of use of the app

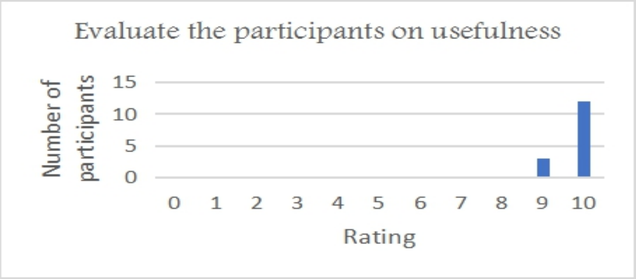


Fig. 19.b Participants ‘evaluation on usefulness

7. Conclusion

In this search, we aimed at exploring the current practices of using mobile devices and the awareness of Saudi Arabian students about personal data on mobile devices. The survey was conducted with 447 high school and higher education students. We found that social networking and messaging were the key use cases of mobile devices. In addition, the study found that more than 95% of higher education students (both male and female) used locks on their phones. However, it was surprising that nearly 87% of high school students (both male and female) also used lock on their phones, even though high school students did not feel as much concern about the privacy of their personal information. Moreover, to investigate their awareness of lock mechanisms we found that privacy was the key factor behind using biometrics. Our survey confirmed our assumption that fingerprint recognition is the most common practice among students. Furthermore, most participants agreed that mobile phones should not be shared due to the fear of exposing personal photos and information. However, it was also discovered that a majority of respondents were willing to chat with unknown people online and a considerable number of those participants opened URLs sent from strangers at least once, which posed a potential threat to their personal data. It was also found that different percentages among our participants have faced the theft of their data, including photos, personal identity information, or social media account information when they open suspicious URLs (phishing attacks). This finding motivated the second key contribution of our research, which is Suspicious URL Detector, a system to help detect suspicious URLs. In fact, we proposed and developed a system to support URL verification on mobile platforms. Our system contains a proof of concept Android mobile app (the same concept can be applied to build an iOS app) and a backend server that fetches URL blacklist data from PhishTank. Our correctness evaluation showed that our system’s performance is very close to Google’s Transparency Report service and surpasses the available comparable mobile apps on the Google Play Store. Our usability study confirmed that our system is easy to use. Moreover, the participants believed our system was useful for protecting user data from phishing on mobile platforms.

Future work

our study showed a number of user behaviors that could be the cause of security attacks or breaches, including poor awareness of changing default application settings, confidence in the application provider, and mobile connectivity to open Wi-Fi networks. As is the case with many cybersecurity attacks, criminals are ahead of the curve when it comes to exploiting vulnerabilities and defences. There is a strong need for future research across all cybersecurity topics, including phishing.

Acknowledgments

The authors would like to thank Umm Al-Qura University (UQU) for all motivation and support to this research .Thanks also for Al-Jouf University for this wonderful graduate studies cooperation giving (Alanood Alenizi) the chance to continue her MS research in the field of information security at UQU.

References

[1] https://www.phishtank.com

[2] Aldhafferi, N., Watson, C., & Sajeev, A. S. M. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. International Journal of Security, Privacy and Trust Management, 2(2).

[3] APWG: Phishing activity trends report Q4 2018. (2019). Computer Fraud & Security, 2019(3), 4. doi:10.1016/s1361-3723(19)30025-9.

[4] Lee, S. & Kim, J. (2013). Warningbird: A near real-time detection system for suspicious URLs in Twitter stream. IEEE Transactions on Dependable and Secure Computing, 10(3), 183-195.

[5] Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. In Proceedings of the 16th International Conference on World Wide Web, 649-656.

[6] Weichao Wang, & Cheng Cui. (2008). Achieving configural location privacy in location-based routing for MANET. MILCOM 2008 - 2008 IEEE Military Communications Conference. doi:10.1109/milcom.2008.4753612.

[7] Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C-M., Karat, J., & Trombeta, A. (2010). Privacy-aware role-based access control. ACM Transactions on Information and System Security, 13(24).

[8] Bünnig, C. & Cap, C. H. (2009). Ad hoc privacy management in ubiquitous computing environments. Second International Conference on Advances in Human-oriented

and Personalized Mechanisms, Technologies, and Services, 85-90.

[9] Taheri, S., Hartung, S., & Hogrefe, D. (2010). Achieving receiver location privacy in mobile ad hoc networks. 2010 IEEE Second International Conference on Social Computing. doi:10.1109/socialcom.2010.122

[10] Economides, A. A. & Grousopoulou, A. (2008). Use of mobile phones by male and female Greek students. *International Journal of Mobile Communications (IJMC),* Vol. 6, No. 6, pp. 729-749, Inderscience. ISSN (Online): 1741-5217, ISSN (Print): 1470-949X. [H-Index (based on Harzing's Publish or Perish software) = 22 (2003-2007); cites per paper = 7.02 (2003-07); SJR= 0.081 (2007); H-Index (based on Scopous) = 12 (2007); acceptance rate = 20%; 'C' journal in Australian Ranking of Journals (2009)].

[11] Leung, L., & Wei, R., (2000). More than just talk on the move: Uses and gratifications Light, R. J., Singer, J. D., & Willet, J. B. (1990). By design: Planning research on higher education. Cambridge, MA: Harvard University Press.

[12] Sun, H. (2004). New chocolate, new technology: Mobile text messaging and youngTaddicken, M. (2014). The 'Privacy Paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of selfdisclosure. Journal of Computer-Mediated Communication, 19(2): 248-273.

[13] Peters, O., Almekinders, J., van Buren, R., Roy, S., & Wessels, J. (2003). Motives for SMS use. Paper presented at the 53rd Annual Meeting of the International

[14] Iqbal, Z. (2010). Gender differences in mobile phone use: What communication motivesit? Retrieved from Oracle Dyn: https://dyn.com/blog/influencer-the-case-for-dmarc-isclear- so-why-doesnt-everyone-use-it/

[15] Lo, J. (2010). Privacy concern, locus of control, and salience in a trust-risk model of information disclosure on social networking sites. AMCIS 2010 Proceedings.

[16] Gross, R. & Acquisti, A(2009). Information revelation and privacy in online social networks. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 71-80.

[17] Zukowski, T. & Brown, I. Examining the influence of demographic factors on internet users' information privacy concerns. Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, 197-204.

[18] McAndrew, F. T. & Jeong, H. S. (2012). Who does what on Facebook? Age, sex, and relationship status as predictors of Facebook use. Computers in Human Behavior, 28(6),2359-2365. doi: 10.1016/j.chb.2012.07.007

[19] Le, A., Markopoulou, A., & Faloutsos, M. (2011). PhishDef: URL names say it all. Proceedings IEEE INFOCOM.

[20] Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 581-590.

[21] Lord, N. (2019). Phishing attack prevention: How to identify & avoid phishing scams in 2019. DigitalInsider. Retrieved from https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams .

[22] Vayansky,l.& Kuma,S.(2018). Phishing – Challenges and Solutions. Elsevier Science Limited, Retrieved from https://www.researchgate.net/publication/322823383_Phishing_-_challenges_and_solutions

[23] https://play.google.com/store/apps/details?id=com.smiilee.acerpc.safesearchbrowser

[24] https://play.google.com/store/apps/details?id=free.phishing.seminarapp

[25] Powers, D.M., 2011. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation.

Alanood Alenizi is a graduate student in Computer Sciences &Engineering from Umm Al Qura University (UQU). Her MS program UQU is specialized in the information security track offered by College of Computer and Information systems offered at UQU-Makkah Campus, Saudi Arabia.

Esam Khan is currently the vice dean for academic affairs at the Custodian of the Two Holy Mosques Institute of Hajj & Umrah Research, and an associate professor in computer engineering at Umm Al-Qura University, Makkah, Saudi Arabia. He received his B.Sc. in Computer Engineering in June 1999, and his M.Sc. in Computer Engineering in June 2001, both from the Department of Computer Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia. He received his PhD in Electrical and Computer Engineering in November 2005 from the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada. His M.Sc. thesis was about compression techniques of testing data. His Ph.D. dissertation was about hardware implementation of hash functions. His research interests include Systemon-Chip (SoC) designs, hardware implementations of security and cryptographic algorithms, steganography techniques, and smart systems design and deployment. He published several journal and conference papers in the areas of his research.