https://doi.org/10.52326/jss.utm.2022.5(3).11
UDC 343.72:004.738.5(669)

CONNECTION TO THE USE OF FREE ANDROID APPS IN KEBBI STATE, NIGERIA

Zauwali Sabitu Paki[1*], ORCID: 0000-0002-3150-6982,
Shamsu Sani[2], ORCID: 0000-0001-6099-405X,
Gambo Isah Diri[2], ORCID: 0000-0003-0333-5909

[1]*Yusuf Maitama Sule University, 800001, Kano, Nigeria*
[2]*Kebbi State Polytechnic Dakingari, 860001, Kebbi, Nigeria*
*Corresponding author: Zauwali Sabitu Paki, *zspaki@yumsuk.edu.ng*

Received: 06. 27. 2022
Accepted: 08. 14. 2022

Abstract. In this paper, we studied scamming emanating from the use of free Android apps by conducting an online survey with respondents recruited from four tertiary institutions in Kebbi State, Nigeria. We found that the apps used for communication, such as Facebook and WhatsApp, have the highest number of users. Also, 55.26 % of users reported receiving scam messages that could be linked to their use of free apps, whereas 32.45 % of them were indeed defrauded by scammers. The study concludes that the free social media apps coupled with the characteristic of the users' login credentials could be responsible for the high rate of scam messages that the respondents receive regularly.

Keywords: *Scamming, respondents, privacy-sensitive data, authentication, users, android operating system, security updates.*

Rezumat. În această lucrare a fost studiată înșelăciunea care provine din utilizarea aplicațiilor Android gratuite, realizând un sondaj online cu respondenți recrutați din patru instituții terțiare din statul Kebbi, Nigeria. Am descoperit că aplicațiile folosite pentru comunicare, precum Facebook și WhatsApp, au cel mai mare număr de utilizatori. De asemenea, 55,26 % dintre utilizatori au raportat că au primit mesaje înșelătorii care ar putea fi legate de utilizarea aplicațiilor gratuite, în timp ce 32,45 % dintre aceștia au fost într-adevăr fraudați de escroci. Studiul concluzionează că aplicațiile gratuite de social media, cuplate cu caracteristicile acreditărilor de conectare ale utilizatorilor ar putea fi responsabile pentru rata mare de mesaje înșelătorii pe care respondenții le primesc în mod regulat.

Cuvinte cheie: *înșelătorie, respondenți, date sensibile la confidențialitate, autentificare, utilizatori, sistem de operare Android, actualizări de securitate.*

1. Introduction

The rapid growth in mobile technology adoption gives rise to new mobile marketing and advertisement opportunities [1]. The opportunities range from real-time customer involvement and increased revenues for marketers and advertisers. The level of massive worldwide surveillance is increasing day in and day out. We normally leave traces that can be objectively and systematically recorded each time we use the internet on our smart devices on the visible or invisible web. These recordings can be for economic or security gains. On the invisible web, things like pixels, cookies, "I like" buttons, and so on websites could potentially be used to track and profile all users. The web browsers that we use are unique and can be tracked. For example, as [2] succinctly put:

- Foursquare knows where you are.
- Flickr knows what you are watching.
- Facebook knows what you are doing.
- LinkedIn knows where and with whom you are working.
- Twitter knows what you are saying.
- Amazon knows what you are buying.
- Google knows what you are thinking.

And many more…

This situation can lead to abuse. The key issue is that our citizens can be tracked throughout the world, compromising the security of our tools, especially with some android permissions [2]. One serious source of concern is the possibility of establishing a linkage between pieces of information like metro cards, debit cards, cellphone data, and their subjects.

Metadata aggregated over a person’s life tells a story about you. The story is made of facts, but that’s not necessarily true.

In our daily life, smart devices are our companions; they are very useful, always connected, and easy to customize. But these devices concentrate personal information (PI) when we use them: phone calls, short message system (SMS), web, applications, etc. Facilities such as global positioning systems (GPS), near field communication (NFC), WiFi, camera, fingerprint sensor, and heart rate sensors generate personal information. So, smartphone knows a lot of our cyber-activities on the internet and our centers of interest through the list of installed applications.

Some actors are interested in people’s wealth of personal information for economic/financial or security gains. This is an ecosystem that centers around Advertising & Analytics (A&A) companies. They serve as an interface between developers, users, and advertisers. Through applications, A&A companies collect PI (e.g., geolocation and technical identifiers), create, and incrementally improve the accuracy of user profiles. From these user profiles, they lunch Real-Time Bidding (RTB) informing those that might be interested in those profiles and consequently send and display targeted advertisements with those applications. A&A companies get a lot of revenue from targeted advertising. For example, Alphabet Inc (owner of Google) said that it earned $ 22.7 billion from advertising [3,4].

This situation is even more worrisome with the improvement in technology in recent times. Things like smartphone payment, wearable connected objects, home connected appliances, connected cars, IoT, etc.

The situation can lead to encroaching on the security and privacy of users. For example, in June 2016, the Federal Trade Commission of the USA fined InMobi (a Singapore-based mobile advertising company) $950,000 for tracking several millions of customers including children without their consent [5]. Our people are likely unaware of this situation. There is a need to create awareness about how best to use these devices.

Android operating system is the most popular and highly used operating system (OS) [2,6,7] with active over 2.5 billion users in over 190 countries [8]. Android operating system comes with permissions systems that give controls to the users [7] to decide whether or not to grant permission needed by an app. Installing Android apps means the user accepts the apps' permissions for their running [2].

On the privacy-sensitive permission, [2] researched the use of ACCESS_WIFI_STATE permission by the popular applications on the Google Play Store. The authors conducted static and dynamic analyzes and discovered that this permission is being used to collect and transmit Personally Identifiable Information (PII) to third-party companies to track and send targeted advertisements. By conducting a survey, the authors also discovered that the majority of users largely underestimated the power of this permission. In the same vein, Ryan, *et al.* [9] conducted research on the use of permissions in ad libraries and discovered that they checked for permissions beyond those listed as required and those listed in their documentation. These included even highly privacy-sensitive and dangerous ones like CAMERA, WRITE CALENDAR and WRITE CONTACTS. The authors found that users can be tracked via the use of those ad libraries. Analysis conducted by [7] about the usage of the Android permissions system revealed indicated an increment of 73.33% which may mean an increase in users' tracking and disclosure of their sensitive data.

Users' awareness of the sensitivity and implication of some Android permissions will help minimize the potential dangers that they might be exposed to. [6] conducted a massive online survey to determine the level of users' awareness of the Android permissions system. The results of the survey indicated a weak level of awareness concerning the privacy of users' data. [10] conducted a controlled online experiment on Android phone users about their perception and awareness of ad libraries and permissions. The authors discovered that improving their level of awareness changed their perceptions and how they make better decisions on their privacy when installing Android apps. [11] built a knowledge base mapping between API calls and fine-grained privacy-related behaviors. They developed an application that enabled Android users to make informed decisions about their privacy when installing an Android application. The authors used the feedback generated from the users of this app and discovered that increasing the users' level of awareness greatly helped them in making wise decisions when installing Android applications.

Therefore, we aim to investigate the following: (1) the rate of scamming (2) the kind of free apps that are mostly used by our people, and (3) peoples' level of awareness about the android permission system. We have the following specific objectives: (1) to determine the type of free applications the targeted users use frequently and (2) to assess the level of people's knowledge about apps authorizations/permissions to access key elements on their phones and the associated implications (3) to ascertain the number of people defrauded due to scamming

2. Materials and Methods

We conducted a 3-month online survey to get data from the targeted respondents by creating a google form available at *https://forms.gle/fGcU4UNzfPVdhhAGA*. The period of the questionnaire was between March 1 and May 20, 2022. A total of 114 respondents volunteered and filled the online questionnaire out of which 91 (79.80%) were males and 23 (20.20%) were females. The respondents were staff and students of 4 high institutions in Kebbi State, Nigeria. The institutions are Federal University Birnin Kebbi (FUB), Kebbi State University of Science and Technology, Aleiro (KSUST), Waziri Umaru Polytechnic Birnin Kebbi (WUPB), and Kebbi State Polytechnic Dakin-Gari (KSPOL). We shared the link to the form via WhatsApp forums of these institutions and members used the link to submit their responses.

3. Results

An online survey questionnaire was administered to the staff and students of six high institutions in Kebbi state, Nigeria. The following subsections present the results of the survey. Figure 1 shows the number of respondents from the selected institutions.

3.1 Distribution of respondents based on their institution

Figure 1 gives the distribution of respondents according to their institutions.

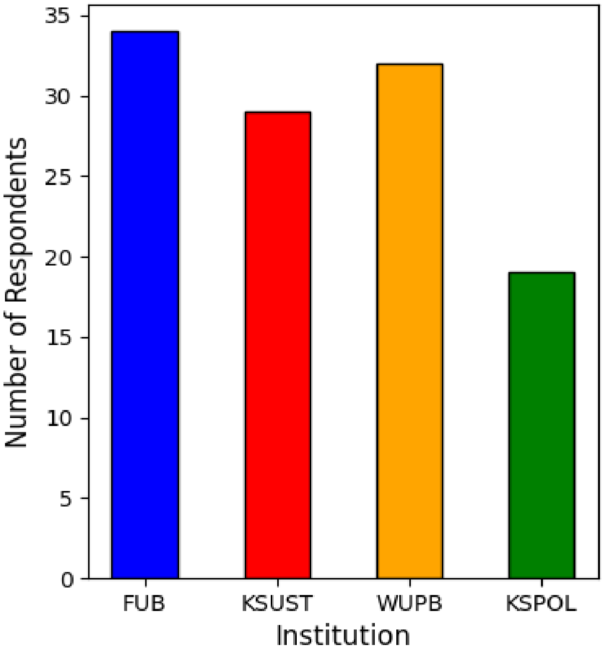

Figure 1. Number of respondents from the selected high institutions.

The recruitment process of the respondents was done by sharing a link to the online questionnaire on the WhatsApp platforms of the selected institutions. We solicited for volunteers to fill out the questionnaire and, as can be seen from Figure 1, we got volunteers from all 4 selected institutions. Federal University Birnin-Kebbi (FUB) had 34 (29.80%) respondents, being the highest, followed by Waziru Umaru Polytechnic Birnin-Kebbi (WUPB) with 32 (28.10%) respondents, then Kebbi State University of Science and Technology (KSUST) with 29 (25.40%), and lastly the Kebbi State Polytechnic with 19 (16.70%) respondents. It is not surprising to have more volunteers from FUB and WUPB than from KSUST and KSPOL as FUB and WUPB have large populations than KSUST and KSPOL.

More so, we chose these institutions because of their heterogeneous nature. FUB and WUPB are federal institutions and hence have staff and students from all parts of Nigeria. KSUST and KSPOL are Kebbi State-owned institutions with staff and students from every nook and cranny of the State

3.2 Major categories of apps most frequently used

We categorize the apps most frequently used by the respondents into 4 categories. The four categories are shown in Figure 1 with the percentage of respondents using them.

The majority of android apps on the Google Play Store fall under one of the categories presented in Figure 2.

The survey reveals that respondents use communication apps more than apps in other categories (approximately 72.2% of the respondents).

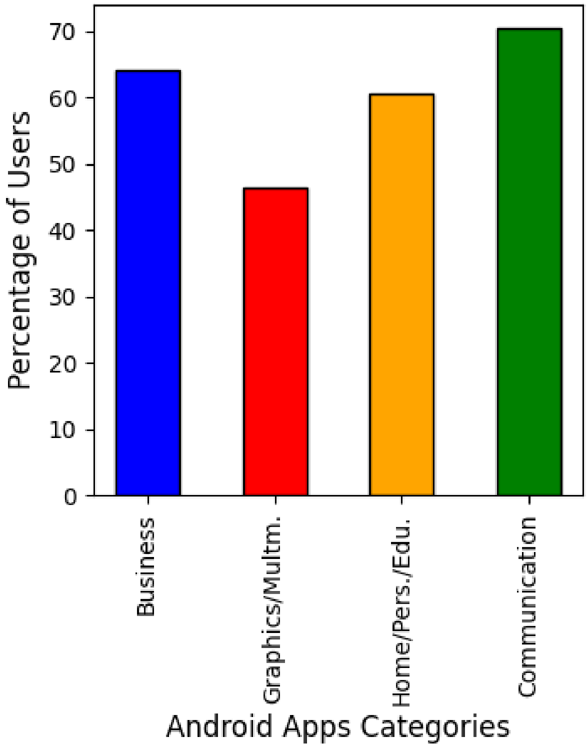

Figure 2. Broad categories of apps and the percentage of respondents using them.

These are apps such as Facebook, WhatsApp, and Instagram. They are used to communicate and create social links and collaborations between friends, colleagues, associates, and members of a community. Sadly, social media apps are leveraged by malicious persons to lure and steal the personal identity of innocent people [12]. The rate of scamming attempts experienced by the respondents may not be unconnected to their use of social media apps like Facebook [13] and dating apps, WhatsApp, and so on. Research conducted by [14] revealed that victims of scamming via social media and online dating apps lose huge amounts of money in addition to the psychological trauma inflicted on them. We can rightly say, as shown by other works, that some social media apps are used as a tool for scamming people by malicious people.

The business apps category is next with approximately 64.04% of respondents using them. Apps in this category include banking and online shopping apps (e.g., Amazon, Jumia).

However, the Home/Personal/Education apps category comprises apps for games, tutorials, etc. We found that about 60.53% of the respondents use them.

3.3 Android versions used by respondents

Here, all respondents using Android version 5 and older are put in one category because they are considered outdated by Google [15]. This is shown in Table 1 below.

Table 1

Android versions and the number of respondents using them

Version	Number of users	Percentage
Android 13	04	03.51
Android 12	08	07.02
Android 11	12	10.53
Android 10	25	21.93

Continuation Table 1

Pie (version 9)	10	08.77
Oreo (versions 8.0 & 8.1)	10	08.77
Nougat (version 7)	03	02.63
Marshmallow (version 6)	07	06.14
Version 5.0 and older	35	30.70

3.4 Nature of access controls used by respondents

We studied the characteristics of access credentials that respondents used to secure access to their phones and installed apps. Note that the security of electronic gadgets such as smartphones lies in the strength of access control credentials used. We have, therefore, studied some aspects that could either strengthen or weaken the amount of security that access credential provides.

On this note, we found that 50.4% of the respondents use part of their phone number (like the first or last 4 digits. See figure 3) as their PIN to unlock their phones and only 44.6% of them regularly change their PINs (e.g., every 3 months as suggested by security experts).

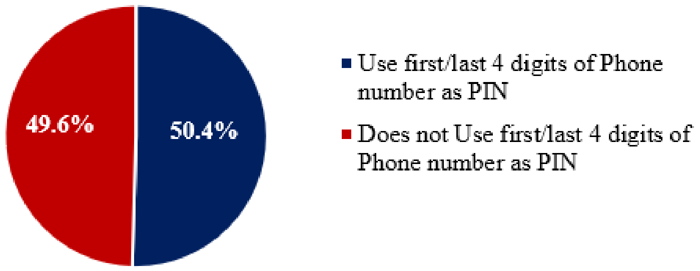

Figure 3. Use of part of a phone number as PIN by respondents.

3.5 Characteristics of access credentials of respondents for frequently used Apps

On the use of a single login credential for all the commonly used apps by the respondents (e.g., banking apps, Facebook, email, etc.), we found that 48.7% use the same login details across all apps they use. Also, 38.1% of them use the names of their family members (such as child, wife, or husband name) as their login details to those apps. More so, on increasing the robustness of a password by making it contain letters, digits, and special characters; only 51.3% do that while the remaining 48.7% either do not comply with this requirement or comply only when it is mandatory.

On the size of their PIN/passwords and how they keep them safe, figures 4 and 5 summarize the result.

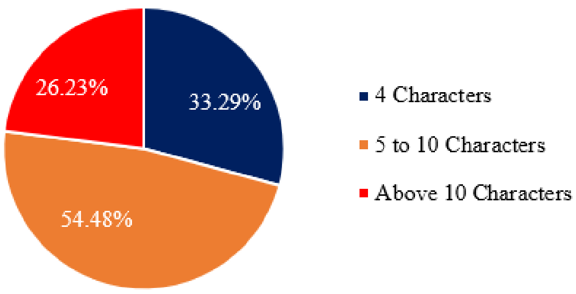

Figure 4. Sizes of PIN/password of respondents.

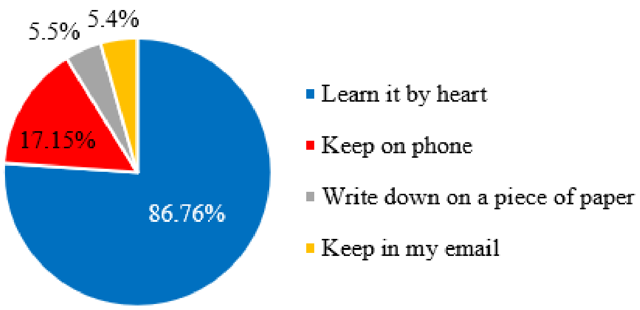

Figure 5. How do users keep safe their login details.

From figure 5, we can see that 28.4% of respondents resort to weaker means of keeping their login credentials by writing them on a piece of paper, saving on the phone, or keeping them on their email.

3.6 Android pattern lock system

The level of security that a pattern lock system provides depends on the complexity of the user's pattern. This directly affects the ease/difficulty with which it can be deduced or learned by a scammer. Complex patterns drawn with lines crossing each other are likely to be more secure and robust to shoulder attacks than simple ones; probably just creating a simple linear line. We found that 53.51% of respondents that use pattern locks on their phones use simple patterns forming lines that do not cross each other.

However, the Android pattern lock system requires a user to use at least 3 points/dots when creating a pattern. Table 2 summarizes the distribution of the number of dots used by respondents.

Table 2

Distribution of dots used by respondents in creating Android pattern lock

Number of Dots Used	Number of Users	Percentage
3	31	27.19
4	24	21.05
5	10	08.77
6	19	16.67
7	6	05.26
8	6	05.26
9	18	15.79

3.7 Attempts to defraud users via SMS and apps ads

A large percentage (55.26%) of respondents confirmed that they receive unsolicited SMSs and targeted ads via the free apps they have installed on their Android phones. It is worthy of note that we discovered that scammers attempted to defraud approximately 85% of the respondents. More worrisome is the fact that 32.45% were indeed tricked and defrauded.

3.8 Respondents' knowledge about Android permission system

We discovered that 69.30% of the respondents have a vague idea about the Android permission system. They do not know the technical detail and the rationale behind it; they only believe it is a requirement that must be fulfilled when installing/using some apps. The remaining 30.7% do not at all know anything about it. More so, 42.1% of them do not even care to read through permission request message that pops up when installing/using apps. They just grant the requested permission without reading it.

3.9 Respondents' perception of free Android apps

About 65% of the respondents believe that free Android apps are created to help people only or to help people and make money. This is shown in table 3 below.

Table 3

Respondents' perception of free Android apps

Reason for free Android apps	Number of respondents	Percentage
To help people only	21	18.42
To help people but also to make money	52	45.61
To trick and defraud people	07	06.14

Continuation Table 3

For fun/hobby	13	11.40
Not sure	16	14.04
Undecided	05	04.39

3.10 Respondents' perception of Android permission system

About 88% of the respondents believe that the Android permissions system is just a requirement by some apps before they can be installed.

3.11 Regular updating of Android system

Updating the Android system regularly is highly recommended to make a phone up to date and secure. Google releases patches and security updates regularly. Many phones receive notifications about the release while others (especially those running older versions of Android OS) do not. In this case, users must manually check, download, and install them. This survey found that 31.8% of respondents do not update their phones regularly. This puts them at risk of many threats.

4. Discussion

We can see from Figure 2 that all Android apps can fall into one for categories. The Communication category (all social media apps fall under this category) has the highest number of users. This could be one of the reasons for the high rate of scamming attempts experienced by the majority of the respondents. Social media apps have gained wider acceptance in recent years as they serve as the quickest and fastest medium for cheaper means of communication and dissemination of information. On the other hand, they are being used by cybercriminals to carry out their illicit activities. This means a user of these apps needs to be wary of cyber criminals and take necessary measures to protect themselves. One of these measures is the use of strong and unbreakable login credentials [16,17]. In this regard, we can see that 50.4% (Figure 3) of the respondents that took part in the survey used part of their phone number as their PIN as shown in figure 3. This is a weak security/privacy policy. If their phone numbers are known, access to their phones and the installed apps might be successful by a criminal. This indicates that their level of awareness is low. This can result in the theft of sensitive data, like contacts [18].

Android system provides some layer of protection to the user by detecting and exposing suspicious apps to the user. This largely depends on the version of the Android system running on the user's phone. Phones that run the recent version of the Android system receive updates and bug fix notifications regularly. Phones that run older versions of the Android system may not receive updates and, therefore, their security is not guaranteed. We have seen a non-negligible percentage of users using the outdated Android operating systems (30.7% from Table 1). The security of these phones cannot be assured as they cannot receive updates from Google. Google indicated that it cannot guarantee the security of outdated Android OSes [15].

The android permission system is meant to accord some level of security control to the phone user. It mandates that any app that intends to access some part of the user's phone (like contacts, gallery, etc.) declare that in the app's manifest file [19]. This requirement is enforced by the Android OS during app installation. It permits the user to review the requirements of an app before installing it. In this respect, the majority of the respondents have a very vague idea about the Android permissions system and believe that it is a mere requirement that needs to be fulfilled when installing some apps (see subsection 3.8). This means that they cannot adequately comprehend and make an informed decision about handling app permission requests.

On the attitude of the respondents towards keeping their phones up to date, it is a bit impressive that 68.2 % of the respondents regularly update their phones as against the 31.8% that do not. But it is still not enough as it is expected that all Android users keep their phones up to date to minimize the risk of malicious apps. So, regular checking for updates and security patches, and installing them on the users' phones is a recommended practice [20].

However, their attitude to how they protect their login detail, we can see from Figure 5 that about 86.76% of them try to memorize their login details. This is impressive. But this is not enough considering the fact a reasonable percentage of them resort to using weak authentication credentials, as highlighted by subsections 3.4 and 3.5. Two-factor scheme gives additional layer of security [21] and helps in cubing scamming attempts by ensuring only an authorized person is able to make any changes to the login detail of a given app.

Android pattern locking system is another mechanism used by the Android OS to provide secure access to smartphones. From Table 2, we can see that 51.76% of the respondents used a pattern that was formed using 5 or more dots out of the 9 dots available. The use of 5 or more dots can help in creating complicated patterns that can avert smudge [22] and shoulder attacks.

More so, we found that more than half of the respondents were lured by scammers whereas a great number of them were indeed defrauded.

5. Conclusions

We would like to conclude by providing the following recommendations: 1) Users need to be careful about the free apps they install on their phones. They should only download and install verified and trusted apps from the Google Play Store. 2) Users should carefully read and analyze the permission request messages that pop up from those apps when installing them. Blindly granting permissions to an app by the users may amount to accessing users' data and could lead to users' privacy leaks. 3) Users should not tap or click on any links that pop up in those free apps that look suspicious or from an unknown source. 4) Users should activate the two-factor authentication option on all apps that have it so that they will be promptly notified of any attempts to modify login parameters on those apps. Especially in apps used to perform financial transactions, two-factor authentication will enable the users to receive a one-time password that is valid for a short time and this adds a layer of security. 5) Users should always use strong passwords comprising both upper- and lower-case letters, special characters, and at least 8-character long. Users should avoid any of their previously used passwords, and update them frequently not use part of their login name as a password. 6) Users should regularly be downloading updates and bug fixes so that they run the latest and secure version of the android system. 7) Users should be switching off their mobile data whenever they are not using it. 8) Users should avoid keeping their phone geolocation always on to obfuscate attempts to record their location for tracking. 9) Users should not respond to any unsolicited messages received on their phones via those free apps. 10) There is a need for greater and wider user awareness campaigns on how best to select and set login details in our society by the Nigerian government.

Acknowledgments. This work was supported by the Tertiary Education Trust Fund (TETFund) via the Institution Based Research (IBR) 2021 for Kebbi State Polytechnic Dakingari.

Conflicts of Interest. The authors declare no conflict of interest.

References

1. Deng, L.; Gao, J.; Vuppalapati, C. Building a Big Data Analytics Service Framework for Mobile Advertising and Marketing. In Proceedings of the 2015 IEEE First International Conference on Big Data Computing Service and Applications, Redwood City, USA, 2015; pp. 256 - 266.
2. Achara, J.P.; Cunche, M.; Roca, V.; Francillon, A. WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission. In Proceedings of the 2014 ACM conference on Security and Privacy in wireless & mobile networks, Oxford United Kindom, 2014.
3. Alphabet. Alphabet Announces Second Quarter 2017 Results. 2017.
4. ZDNet. Quarterly: Alphabet's Turnover up 21% Despite EU fine. Available online: https://www.zdnet.fr/actualites/trimestriels-le-ca-d-alphabet-en-hausse-de-21-malgre-l-amende-de-l-ue-39855362.htm (accessed on 17th August 2021).
5. FTC-USA. Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission. Available online: https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked (accessed on August 10 2021).
6. Alani, M.M. Android Users Privacy Awareness Survey. *International Journal of Interactive Mobile Technologies* 2017, *11*.
7. Almomani, I.M.; Khayer, A.A. A Comprehensive Analysis of the Android Permissions System. *IEEE Access* 2020, 8, pp. 216671 - 216688, doi:10.1109/ACCESS.2020.3041432.
8. Curry, D. Android Statistics 2022. Available online: https://www.businessofapps.com/data/android-statistics (accessed on 20/05/2022).
9. Ryan, S.; Clint, G.; Jon, C.; Jeremy, E.; Hao, C. Investigating User Privacy in Android Ad Libraries. In *Proceedings of the Workshop on Mobile Security Technologies (MoST)*, 2012; pp. 195-197.
10. Na, W.; Bo, Z.; Bin, L.; Hongxia, J. Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. In *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services*, Copenhagen, Denmark, August 24–27, 2015, 2015; pp. 373-382.
11. Sanae, R.; Zhiyun, Q.; Morely, M.Z. Appprofiler: A Flexible Method of Exposing Privacy-Related Behavior in Android Applications to End-Users. In *Proceedings of the ACM conference on Data and application security and privacy*, 2013; pp. 221-232.
12. Majeed, A.; Zia, H.; Imran, R.; Saleem, S. Forensic analysis of three social media apps in windows 10. In *Proceedings of the 2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET)*, 2015; pp. 1-5.
13. Patel, P.; Kannoorpatti, K.; Shanmugam, B.; Azam, S.; Yeo, K.C. A theoretical review of social media usage by cyber-criminals. In *Proceedings of the 2017 International Conference on Computer Communication and Informatics (ICCCI)*, 2017; pp. 1-6.
14. Coluccia, A.; Pozza, A.; Ferretti, F.; Carabellese, F.; Masti, A.; Gualtieri, G. Online romance scams: relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health: CP & EMH* 2020, 16, p. 24.
15. Razaghpanah, A.; Niaki, A.A.; Vallina-Rodriguez, N.; Sundaresan, S.; Amann, J.; Gill, P. Studying TLS Usage in Android Apps. In *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*, Incheon, Republic of Korea, December 12 - 15, 2017, 2017; pp. 350-362.
16. Ye, B.; Guo, Y.; Zhang, L.; Guo, X. An empirical study of mnemonic password creation tips. *Computers & Security* 2019, 85, pp. 41-50.
17. Shen, C.; Yu, T.; Xu, H.; Yang, G.; Guan, X. User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security* 2016, 61, pp. 130-141.
18. Yang, Z.; Yang, M.; Zhang, Y.; Gu, G.; Ning, P.; Wang, X.S. Appintent: Analyzing sensitive data transmission in android for privacy leakage detection. In *Proceedings of the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013; pp. 1043-1054.
19. App Manifest Overview. Available online: https://developer.android.com/guide/topics/manifest/manifest-intro (accessed on 20/06/2022).
20. Samteladze, N.; Christensen, K. DELTA++: Reducing the Size of Android Application Updates. *IEEE internet computing* 2013, 18, pp. 50-57.
21. Aloul, F.; Zahidi, S.; El-Hajj, W. Two factor authentication using mobile phones. In *Proceedings of the 2009 IEEE/ACS international conference on computer systems and applications*, 2009; pp. 641-644.
22. Aviv, A.J.; Gibson, K.; Mossop, E.; Blaze, M.; Smith, J.M. Smudge attacks on smartphone touch screens. *In Proceedings of the 4th USENIX Workshop on Offensive Technologies (WOOT 10)*, 2010.

Citation: Paki, Z.S.; Sani, S.; Diri, G.I. Connection to the use of free android apps in Kebbi state, Nigeria. *Journal of Social Sciences* 2022, 5 (3), pp. 144-154. https://doi.org/10.52326/jss.utm.2022.5(3).11.

Publisher's Note: JSS stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright:© 2022 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license
(https://creativecommons.org/licenses/by/4.0/).

Submission of manuscripts: jes@meridian.utm.md