ISSN No:-2456-2165

Free Android Apps vs. Users' Privacy: A Case Study of Some Selected Tertiary Institutions in Kebbi State, Nigeria

Zauwali Sabitu Paki
Departement of Computer Science,
Yusuf Maitama Sule University
Kano, Nigeria

Shamsu Sani
Department of Computer Science,
Kebbi State Polytechnic Dakingari,
Nigeria

Gambo Isah Diri
Department of Mathematics,
Kebbi State Polytechnic Dakingari,
Nigeria

Abstract:- The rate of breaches of users' privacy is on the increase in recent times. fraudsters employ several strategies to track, profile, and steal users' Personally Identifiable Information (PII) either for financial or malicious gains. One of these strategies is by sending messages via SMS, ads in the free Android apps, and social media platforms. The success or otherwise of fraudsters largely depends on the strength/weakness of users' access control credentials and their attitudes towards the use of free Android apps. In this work, we study the nature of users' login credentials and their adherence to cybersecurity recommendations. We conducted an online survey with respondents from some selected tertiary institutions in Kebbi state, Nigeria. We focused on the apps that users frequently use and how they keep up-to-date with their login stuff. We found that 48.7% of users use the same pin/password for all their apps. 59.3% and 59.6% of respondents always leave their location and mobile data ON, respectively.

Keywords:- *mobile data; authentication; android operating system; Android permission.*

I. 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]. The possibility of establishing a linkage between pieces of information like metro cards, debit cards, cellphone data, and their subjects is one serious source of concern.

"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., using 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

ISSN No:-2456-2165

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, Clint, Jon, Jeremy and Hao [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 users' attitudes toward free android apps (2) the kind of free apps that are mostly used by our people, and (3) how people operate their phones concerning privacy consciousness. 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.

II. FREE ANDROID APP ECOSYSTEM

A. *Major Actors Involved*

A lot of users do not know the real actors behind the free Android apps that they use. Several actors are involved in the development and deployment of Android apps, ranging from the app developer to the final user. Users do normally get in touch with just one primary actor: the Play Store from which they download and install the free apps. But it is much more than just the Play store. The ecosystem comprises the A&A companies (e.g., AdMob, Flurry, Inmobi, and millennial media), advertisers, Play Store, and App. developer, and the user. This is outlined in fig. 1.

Fig. 1: Actors involved in Android app development and deployment [12]

The app developer builds the app with specifications from the A&A company, which pays the developer. The specifications may comprise embedding AdID in the free app so it can be used for sending targeted ads by the A&A company. A&A is normally a giant organization that builds and improves user profiles and sells them to advertisers. As can be seen from fig. 1, the advertisers pay a huge sum of money to the A&A which in turn advertises their products by sending a targeted advertisement to users via installed free apps. It can also be seen that A&A pays little to app developers

B. *Android Permission System and User Control*

Android platform mandates all apps that need access to some components of the user's phone to categorically indicate that in the apps AndroidManifest.xml file which describes crucial information about the app to the Android build tools, Android operating system, and the Google Play [13]. The workflow for using Android permission is illustrated in fig. 2

ISSN No:-2456-2165

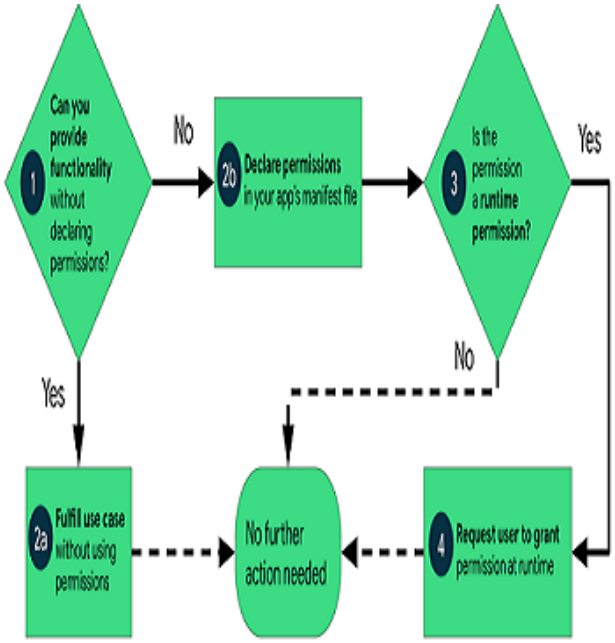

Fig. 2: Workflow for using Android permissions [14]

As indicated in fig. 2 it can be deduced that apps need permission can request so from the user either at installation time or runtime. If the app needs permission at install time, the user may not be able to install the app if s/he denies the permission. This indicates that user needs to be careful about the kinds of permissions to be allowed.

Permission has improved a bit better with one-time permission starting with Android 11 (API level 30). Users can grant permission for just a short time depending on the app's behavior and user's activity. Fig. 3 gives an example of a system dialog that requests one-time permission.

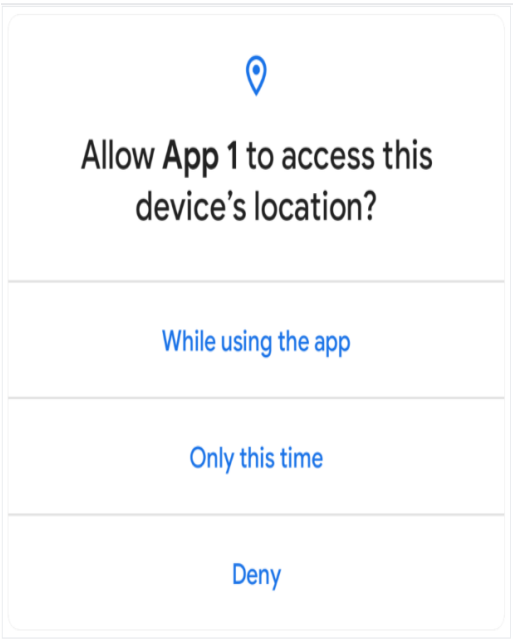

Fig. 3: Example of one-time permission request dialog [14]

III. METHODOLOGY

Our main objective was to examine the potential privacy threats posed emanating from the use of free android apps by the targeted users. We designed an online questionnaire and distributed it on social media platforms of the selected tertiary institutions in Kebbi State. The link to the questionnaire is available at: https://forms.gle/fGcU4UNzfPVdhhAGA.

We had a total of 114 respondents from the four (4) selected tertiary institutions as shown in table 1.

Name of Institution	# Respondents
Federal University Birnin Kebbi	34
Kebbi State University of Science and Technology, Aleiro	29
Waziri Umaru Polytechnic Birnin Kebbi	32
Kebbi State Polytechnic Dakin-Gari	19

Table 1: Respondents and their institutions

The distribution of male and female respondents is 91 and 23 respectively.

We targeted educated people because they can read and understand and hence might know the best practice in terms of smartphone usage as shown in fig. 4.

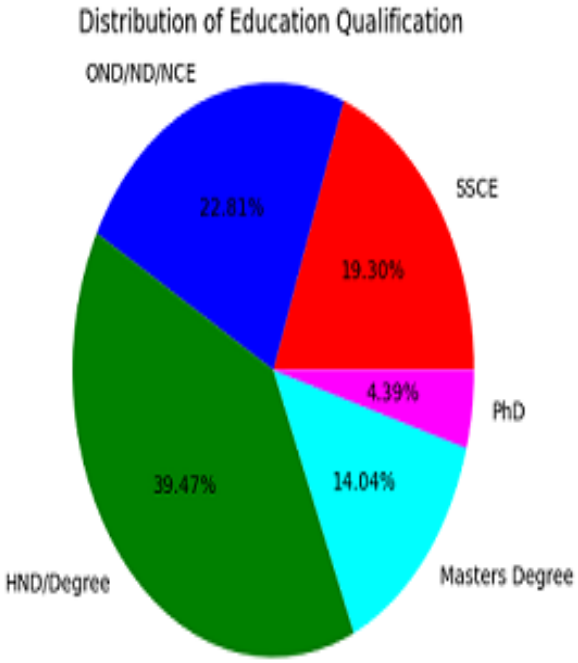

Fig. 4: Distribution of educational qualifications of the respondents

From fig. 4, OND (Ordinary Diploma), ND (National Diploma), and NCE (Nigeria Certificate of Education) are post-high school qualifications. HND (Higher National Diploma) is a qualification equivalent to a university degree awarded by polytechnics. SSCE, on the other hand, stands for Senior Secondary School Certificate.

ISSN No:-2456-2165

IV. RESULT OF THE SURVEY

We now present the result of the survey conducted in this section.

A. *Android Version Used*

To some extent, the level of security of an Android phone depends on the version of the OS used. Table 2 gives this information.

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
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. X and below	35	30.70

Table 2: Android versions installed on respondents' phone

We can see from table 2 that some 30.70% of the respondents use Android 5.0 and below.

B. *Nature of Users' PIN Code*

We surveyed how respondents set PIN codes on their phones. Normally people tend to set PINs that they can easily remember. This makes them resort to using weak PINs. One of the weak PINs is the use of the first/last four digits of one's mobile phone number as a PIN. We discovered that 50.40% of respondents use part of their mobile phone number as their PIN.

C. *Use of Single Login Credential and Size of User's Passwords*

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 5 and 6 summarize the result.

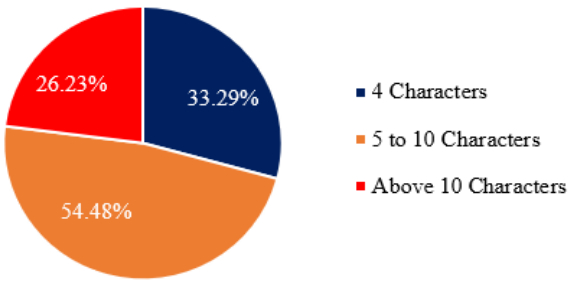

Fig. 5: Sizes of PIN/password of respondents

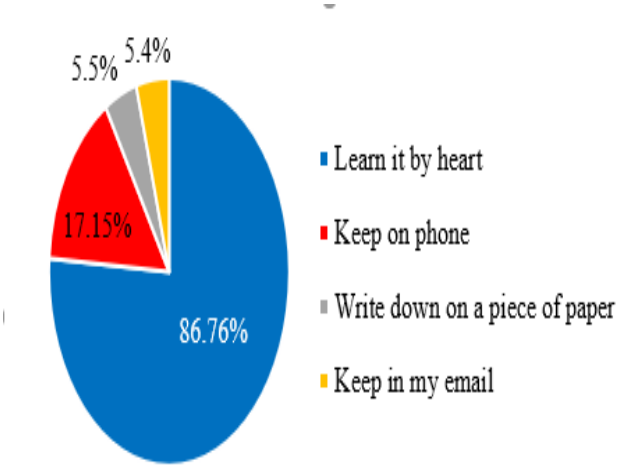

Fig. 6: how users keep safe their login details

D. *Major Apps Used by Respondents*

We categorize the apps most frequently used by the respondents into 4 categories as shown in figure 2.

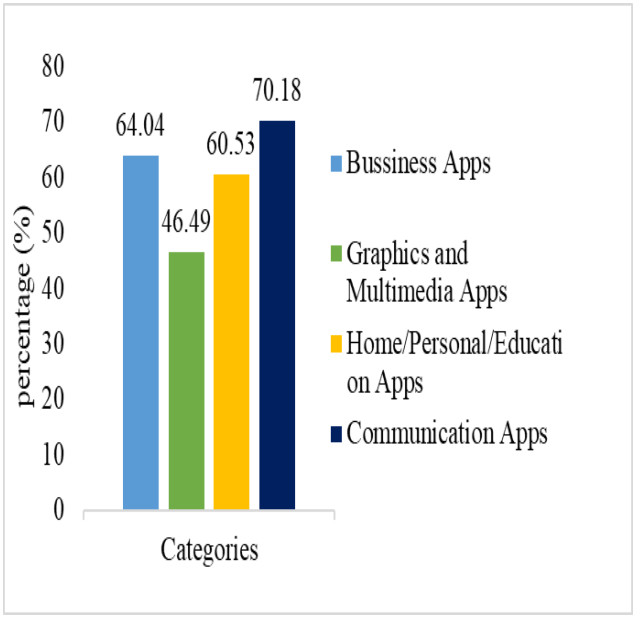

Fig. 7: Categories of Android Apps

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). 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. The business apps category is next with approximately 64.04% of respondents using them. Apps in this category include apps such as banking apps 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.

E. Keeping Location and Mobile Data Always ON

Android phone's location information is crucial to profiling a user. Some free apps gather this information and send it to an A&A company for financial benefits, or some third party for a malicious purpose. A&A company normally aggregates the data as it comes and builds a strong user profile as time goes on. Consequently, it sends targeted adverts to the affected user and, as a result, gets huge money from advertisers. We discovered that 60.20% of respondents set their phone location always on.

Mobile data that is always open, on the other hand, will facilitate the smooth transmission of users' sensitive information to a third party as those apps may require an internet connection to transmit the data they have gathered. In this regard, we found that 59.30% of the respondents keep their mobile data open all the time.

F. Users' Attitudes towards keeping Android Phone Up-to-date

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.

G. Defrauding Users

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.

V. DISCUSSION

We can see that 50.4% of the respondents that took part in the survey used part of their phone number as their PIN. This is a weak security/privacy policy. If their phone numbers are known, access to their phones is just guaranteed. We can, therefore, deduce that majority of the respondents have inadequate knowledge about what constitutes a strong/weak PIN; they bother more about the ease with which they can remember the PIN. Weak access control credentials expose users to vulnerabilities that scammers can exploit. Coupled with the attitudes of the majority of respondents toward leaving their mobile data always ON, users' sensitive data can be transmitted in almost real-time to a third party. This may not be unconnected, as a consequence, with the high rate of scam attempts (55.26% of them were once attempted by scammers) as some research has shown that there are dangerous free apps that steal users' sensitive data, like contacts. We can infer a connection between the level of security a user gets and the version of Android used. We have seen a non-negligible percentage of users using the outdated Android operating systems (30.7%) as they cannot receive updates from Google. Google indicated that it cannot guarantee the security of outdated Android OSes [15].

VI. CONCLUSION

In this work, we studied the strengths/weaknesses of respondents' login details to Android phones about their use of free apps. We found some level of weakness with their login credentials. More so, we found that more than half of the respondents received scammed messages attempting to defraud them by scammers whereas a great number of them were indeed defrauded. It is worrisome to note that all the respondents are educated but still we discovered a low level of awareness in this regard. There is a need for more enlightenment campaigns to educate people in Kebbi State about best practices on using mobile phones and their cyber activities in general.

ACKNOWLEGEMENT

This work was supported by a grant for Institution-based research (IBR) 2021 for Kebbi State Polytechnic Dakingari from the Nigeria's Tertiary Education Trust Fund (TETFund).

REFERENCES

[1.] L. Deng, J. Gao, and C. Vuppalapati, "Building a Big Data Analytics Service Framework for Mobile Advertising and Marketing," in 2015 IEEE First International Conference on Big Data Computing Service and Applications, Redwood City, USA, 2015, pp. 256 - 266.

[2.] J. P. Achara, M. Cunche, V. Roca, and A. Francillon, "WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission."

[3.] Alphabet, "Alphabet Announces Second Quarter 2017 Results," https://abc.xyz/investor/static/pdf/2017Q2_alphabet_earnings_release.pdf, 2017].

[4.] ZDNet. "Quarterly: Alphabet's Turnover up 21% Despite EU fine," 17th August 2021, 2021; https://www.zdnet.fr/actualites/trimestriels-le-ca-d-alphabet-en-hausse-de-21-malgre-l-amende-de-l-ue-39855362.htm.

[5.] FTC-USA. "Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission," August 10 2021, 2021; https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.

[6.] M. M. Alani, "Android Users Privacy Awareness Survey," *International Journal of Interactive Mobile Technologies*, vol. 11, 2017.

[7.] I. M. Almomani, and A. A. Khayer, "A Comprehensive Analysis of the Android Permissions System," *IEEE Access*, vol. 8, pp. 216671 - 216688, 2020.

[8.] D. Curry. "Android Statistics 2022," 20/05/2022, 2022; https://www.businessofapps.com/data/android-statistics.

[9.] S. Ryan, G. Clint, C. Jon, E. Jeremy, and C. Hao, "Investigating User Privacy in Android Ad Libraries." pp. 195-197.
[10.] W. Na, Z. Bo, L. Bin, and J. Hongxia, "Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions." pp. 373-382.
[11.] R. Sanae, Q. Zhiyun, and M. Z. Morely, "Appprofiler: A Flexible Method of Exposing Privacy-Related Behavior in Android Applications to End-Users." pp. 221-232.
[12.] V. Roca, "Privacy and Smartphones," Universite Nice Sophia Antipolis, France, 2020.
[13.] "App Manifest Overview," 20/06/2022, 2022; https://developer.android.com/guide/topics/manifest/manifest-intro.
[14.] A. Developers. "Permissions on Android," 20/06/2022, 2022; https://developer.android.com/guide/topics/permissions/overview.
[15.] A. Razaghpanah, A. A. Niaki, N. Vallina-Rodriguez, S. Sundaresan, J. Amann, and P. Gill, "Studying TLS Usage in Android Apps." pp. 350-362.