ISSN-2347-2227
Subscribers copy
Not for sale

i-manager's

# Journal on Computer Science

Disseminating new ideas in Information and Computation

i-manager® Publications

ISSN-2347-2227
Volume 6. No. 3
September - November 2018

## i-manager's

# Journal on Computer Science

### About the Journal

*i-manager's Journal on Computer Science deals with all aspects of computer science and contributes theoretical results and offers a compilation of high quality articles to encompass a wide spectrum of advancements in the actively developed domain. i-manager's Journal on Computer Science covers a great deal of what has been done in the field recently and intends to bring together the most recent advances and applications in all branches of the academic computer science community with new knowledge and technology for the benefit of students, professionals and industrial practitioners.*

*i-manager's Journal on Computer Science is presently in its 6th Year. The first issue was launched in 2013.*

*i-manager's Journal on Computer Science is published by i-manager Publications, one of India's leading Academic Journal Publisher, publishing 28 Academic Journals in diverse fields of Engineering, Education, Management and Science.*

### Why Publish with us

*i-manager Publications currently publishes academic Journals in Education, Engineering, Scientific and Management streams. All of i-manager's Journals are supported by highly qualified Editorial Board members who help in presenting high quality content issue after issue. We follow stringent Double Blind Peer Review process to maintain the high quality of our Journals. Our Journals target both Indian as well as International researchers and serve as a medium for knowledge transfer between the developed and developing countries. The Journals have a good mix of International and Indian academic contributions, with the peer-review committee set up with International Educators.*

### Submission Procedure

*Researchers and practitioners are invited to submit an abstract of maximum 200 words on or before the stipulated deadline, along with a one page proposal, including Title of the paper, author name, job title, organization/institution and biographical note.*

*Authors of accepted proposals will be notified about the status of their proposals before the stipulated deadline. All submitted articles in full text are expected to be submitted before the stipulated deadline, along with an acknowledgement stating that it is an original contribution.*

### Review Procedure

*All submissions will undergo an abstract review and a double blind review on the full papers. The abstracts would be reviewed initially and the acceptance and rejection of the abstracts would be notified to the corresponding authors. Once the authors submit the full papers in accordance to the suggestions in the abstract review report, the papers would be forwarded for final review. The final selection of the papers would be based on the report of the review panel members.*

### Format for Citing Papers

*Author surname, initials (s.) (2018). Title of paper, i-manager's Journal on Computer Science, 6(3), xx-xx.*

### Copyright



### Contact e-mails

*editor_jcom@imanagerpublications.com*
*submissions@imanagerpublications.com*

ISSN-2347-2227
Volume 6. No. 3
September - November 2018

# i-manager's
# Journal on Computer Science

ISSN-2347-2227
Volume 6. No. 3
September - November 2018

## i-manager's

# Journal on Computer Science



OUR OFFICES

**Registered Office**

3/343,Hill view,
Town Railway Nager,
Nagercoil, Kanyakumari District - 629001
Ph : 91-4652- 277675
E-mail : info@imanagerpublications.com

**Editorial Office**

13-B, Popular Building,
Mead Street, College Road,
Nagercoil, Kanyakumari District - 629001
Ph : (91-4652) 231675, 232675, 276675
E-mail : editor_jcom@imanagerpublications.com

*Abstracting / Indexing*

ProQuest · ULRICHSWEB GLOBAL SERIALS DIRECTORY · Google Scholar · OCLC WorldCat

Join with us

https://www.facebook.com/Journal-on-Computer-Science-2168468313379110/

https://www.facebook.com/imanagerPublishing/

https://twitter.com/imanagerpub

# CONTENTS

## RESEARCH PAPERS

# EDITORIAL

*The current issue of i-manager's Journal on Computer Science mainly focuses on Authentication System, Artificial Neural Network used to detect e-banking Phishing Websites, Password Management, Adaptive Personnel Selection Expert System to Support Organization's Personnel Recruitment Decision Process, Evaluation of Classification Algorithms for Phishing URL Detection and detection of Captcha Smuggling Attacks using Supervised Deep Learning Based Approach.*

*Omorogiuwa and his co-author Aziken have proposed a study about Computer-Based Local Area Authentication System. The system was developed using XAMPP integrated net-base application and JAVA object-oriented programming language. This security system is controlled through the network via the server and controls all clients that choose to use the resources like e-exam platform, e-library, etc. The performance of the system has been monitored and the result is found to be satisfactory, as all unauthorized users are blocked and appropriate warning messages are sent to the client's system by the server when the user attempts to login which eliminates external users from gaining access to the examination platform.*

*Shafi'i Muhammad Abdulhamid et al., have proposed a study about a soft computing approach to detect e-banking phishing websites using Artificial Neural Network (ANN). Confusion matrix analysis was used in this study to detect e-banking phishing websites. Datasets from various websites comprises of both legitimate and phishing websites collected from directory and analysed by ANN Algorithm with Confusion Matrix. The study results showed that the proposed ANN algorithm produces a remarkable percentage of accuracy and reduced false positive rate during detection and can produce competitive results that is suitable for detecting phishing in e-banking websites.*

*Victor N. Adama et al., have presented a study to analyse about password knowledge and password management. This research was conducted via a case study aimed at establishing the theoretical password knowledge in comparison to actual password management practice of staff and students from Information Technology (IT) inclined departments of the Federal University of Technology, Minna. The data collection was carried out primarily based on a survey. The study results concluded that, there is a significant difference between what respondents know compared to their actual practice. The authors recommend that, more extensive research into enhancing graphical password entropies are to be conducted in future as they possess the potential to replace text passwords.*

*Muhammad Ahmad Shehu et al., have proposed a study to analyze the personnel recruitment operation which is an essential human resource operation of an organization. An adaptive personnel selection model was developed to minimize the complexity and to carry out the personnel selection by considering some of the operational behaviors. The adaptive personnel selection model was developed using a C4.5 decision tree and frequent and non-frequent pattern analysis of data mining. The study results showed that, the proposed expert system enables the personnel selection strategy changes to be fed in by the organization, when it occurs.*

*Oluyomi Ayanfeoluwa et al., have conducted a study to evaluate the capacity of different algorithms to detect phishing URLs. Dataset was obtained from UCI Machine Learning Repository, and the algorithms were assessed in terms of Accuracy, Precision, Recall, F-Measure, Receiver Operating Characteristic (ROC) area and Root Mean Squared Error (RMSE). In terms of accuracy, precision, recall, F-measure, and RMSE, the Random Forest algorithm was found to perform better than the other algorithms analyzed and a number of others from existing literature. The authors recommend that, further studies are to be conducted, to ascertain if performances are dataset-specific.*

*Moses O. Omoyele et al., have proposed a study to analyze a predictive model for the detection of captcha smuggling attacks. In order to achieve the aim, framework based on hyper parameter specification was developed in this study. The model was evaluated on the available CAPTCHA smuggling dataset. The outcome of this research will benefit web developers, web users, web hosting companies and internet service providers. The study results showed that, the accuracy of prediction achieved in this work is 77.89% at consistency of 0.1543. The sensitivity and specificity of the model are 78.11% and 78.2%, respectively.*

*All papers of this issue, papers 1 to 6 were submitted from the 2nd International Conference on Information and*

# EDITORIAL

*Communication Technology and Its Applications (ICTA 2018), conducted on 5 -6th September 2018 at Federal University of Technology, Minna, Nigeria. We express our gratitude to the Conveners Dr. Shafii Abdulhamid & Dr. Oluwafemi Osho for their support in ensuring the papers were submitted on time.*

*We extend our sincere thanks to the authors for their contributions towards this issue and we are grateful to the reviewers for spending their quality time in reviewing these papers. Our special thanks to the Editor-in-Chief, Dr. Kamal kumar Mehta for his continuous support and efforts in improving further the quality of the Journal.*

*Enjoy reading!*

*Warm regards,*

*Ramani R*
*Junior Associate Editor*
*i-manager Publications*

# PASSWORD KNOWLEDGE VERSUS PASSWORD MANAGEMENT

By

VICTOR N. ADAMA * NOEL MOSES DOGONYARO ** VICTOR L. YISA ***
BABA MESHACH **** EKUNDAYO AYOBAMI *****

*,***** Lecturer, Department of Computer Science, Federal University of Technology, Minna, Nigeria.
**-**** Lecturer, Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.

Date Received: 11/01/2019 Date Revised: 28/01/2019 Date Accepted: 22/03/2019

***ABSTRACT***

*User authentication is one of the most important security characteristics of any system given today's globalized digital life style. The safety and security of sensitive data, privacy and also critical infrastructure relies primarily on authentication. Amongst all authentication schemes, text-based passwords are the most deployed across various platforms, thus the importance of evaluating user password management practice cannot be overemphasized. This research, via, a case study aimed at establishing the theoretical password knowledge in comparison to actual password management practice of staff and students from Information Technology (IT) inclined departments of the Federal University of Technology, Minna. Results from the survey reveal that the target respondents are knowledgeable on good password management policies. However, actual password practice results by the respondents showed that they do not comply and effectively implement the theoretical password knowledge they possess. Thus it can be concluded that there is a significant difference between what respondents know compared to their actual practice. Numerous implications abound when this is the case as it makes users more vulnerable to security risks of unauthorized access by unauthorized users.*

*Keywords: Authentication, Password, Password Knowledge, Password Practice.*

## INTRODUCTION

In today's digital age, people use the internet for business transactions, leisure and entertainment (social media), academics and many more. This has led to the dependency on computers and other computing devices (such as Smartphones, Personal Digital Assistant (PDA), Tablets, Smartwatches, etc). According to Ritó, "The internet and digital technologies are transforming our world in every walk of our private and commercial lives" (Ritó, 2018). The task of keeping user data secure, either offline or online, is more than ever before of utmost importance. Data must be protected from unauthorized access (hackers, for example), who can steal or manipulate them. One way to achieve this protection is through authentication. Authentication verifies the identity of the acclaimed user. However, there is the challenge in making authentication systems both secure and usable for authorized users. This is a trade-off that must be balanced.

Passwords play a vital role in our day-to-day lives. The traditional and most widely used method of authentication is the use of text passwords (De Angeli, Coventry, Johnson, & Renaud, 2005). Passwords are used by users to gain access to personal computers, email accounts, mobile phones, automated teller machines, bank accounts, work place networks and devices etc. They act as a gateway between the user and their personal information (McDowell, Hernan & Rafail, 2018). Good password policies recommend that users choose strong passwords. When adhered to, it decreases the chances of them easily guessed by unauthorized users. In contrast to these policies, the vast majority of users use weak passwords. In addition, they exhibit practices detrimental to their security. Such practices include writing

passwords down in a book, using the exact same password across multiple accounts (Renaud, Mayer, Volkamer & Maguire, 2013) and many others.

Blanchard, in 2014, revealed that having weak passwords put millions of bank accounts and other financial transactions on the internet at high risk of being hacked (Blanchard, 2014). Helkala and Bakas found that most computer users are still using password that has guessable structure (Helkala & Bakås, 2014), for example, a password that has just words or numbers and no combination of alphanumeric characters. A report by TeamsID in 2016, revealed twenty-five most commonly used passwords (TeamsID, 2016). The top three most commonly used passwords were "123456", "password", and "12345678". Based on the report, further investigation revealed that most of the passwords were just "word" and numeric passwords making them easier to guess by unauthorized users.

## 1. Related Works

Several surveys have been conducted as regard to passwords. An example of such work is that of Stobert, and Biddle. Their work investigated how users cope with password requirements and management issues (Stobert & Biddle, 2014). Also, the work of Notoatmodjo (2007) revealed that if a user has N distinct passwords for each with a bit size log(S), then the user will have to remember not only N x Log(S) bits, but also which of the N! mapping of password to account is correct. This gives a total expected bit size to be remembered of:

$$E(N) * LOG(n!) \quad (1)$$

The factorial term quickly grows large as N increases. This is one of the reasons why many users ignore security advice of having strong passwords to secure their personal data. Also, Notoatmodjo conducted a survey-based research on user passwords (Notoatmodjo, 2007). The research findings revealed that participants reported an average of 12.9 account and 8 passwords. It also revealed that the number of accounts was correlated to the user's number of years of internet experience. The researcher asked users to classify their accounts into high and low importance accounts groups and found that their categorization was related to the length of password, and how they were reused. Another research by Florencio et al. (2014) conducted a survey using 45 undergraduate respondents in which respondents were asked how many passwords they had and how often they reuse their passwords, how they handled Automated Teller Machine (ATM), Point of Sales (PoS), receipts and their knowledge on the use of passwords (Florêncio, Herley, & Van Oorschot, 2014). It was realized that users have a high number of reused passwords. Also, many have been scammed due to improper disposal of their ATM or PoS receipts and that most users rely on memory and passwords reminder features to remember their passwords. Research by Kelley et al. measured password strength against password cracking algorithms, testing the metrics for password creation policies (Kelley et al., 2013).

However, while extensive studies have been conducted on passwords, there has been limited research done regarding the gap between the knowledge and behavior of password management (Fredericks, Futcher, & Thomson, 2016). In order to secure personal and organizational information, users of IT tools need to know the importance of good password management. According to Stobert and Biddle, passwords go through a four phase cycle (Stobert & Biddle, 2014). This includes: creation, storage, maintenance, and deletion. This will be discussed in the following subsection.

### *1.1 Password Creation Phase*

The first line of defense against unauthorized access to vital computer and personal data is to have a strong password. The stronger the password, the lower the chances it will be hacked (Microsoft, 2013). The report showed that strong passwords must adhere strictly to various rules relating to password length and contents. A good password should have a combination of letters, numbers, and symbols.

### *1.2 Password Storage Phase*

According to University of Illinois, using the same password for all accounts is like having one key that unlocks every door in a person's life (University of Illinois, 2014). Using the same password for multiple accounts is disastrous,

because it would not take long for a hacker to identify which sites they can apply their hacked password on. In this regard, users can make use of password managers to store their passwords if they have many passwords that they utilize. A password manager is a database which stores user's passwords and their corresponding user accounts. The danger is that, if a hacker gains access to the master password, then, the hacker would gain full control over all other user account (Chiasson, Forget, Stobert, Van Oorschot, & Biddle, 2009). By implication the master password must be highly secure. Password managers on this part are risky when used. They are no substitution for secure and usable authentication (Renaud et al., 2013).

### *1.3 Password Deletion*

The work of Stobert and Biddle, revealed that most users tend to forget their passwords because they are too difficult to recall. If a user is no longer using an online account, he should delete the account and the corresponding password. When such accounts are left online over a period of time without been used, there is the tendency that a hacker can compromise the account for their selfish gain that could lead to identity theft.

## 2. Research Design

The research was carried out primarily based on a survey. The research aimed at investigating the existence of a gap between password policy knowledge and actual practice by IT users. The target audience in this research is limited to students and staff of the Federal University of Technology, Minna with emphasis on Information Technology inclined departments. However interested members from other departments were allowed to participate. The research simply asked two research questions. First, are users knowledgeable on good password management policies? Secondly, do they put this knowledge into practice? Finally, to investigate the existence of the gap, a comparison between their theoretical knowledge and their actual password practice was carried out. This informed the survey to be structured and categorized into three sections. The first section collected information about the demographics of the respondents and their basic password needs. The second section, sought the respondents to establish theoretical password policy knowledge. Lastly, the third section sought to establish the respondent's actual password behavior and practice.

### *2.1 Demographics*

In this section the survey collected basic information on the respondents and their basic password needs. The questions in Table 1 are labeled using section number and question number, S1Q1 representing Section 1 Question 1.

### *2.2 Theoretical Password Policy Knowledge*

In this section the survey aimed at establishing the respondent's theoretical password policy knowledge. The questions in Table 2 are labeled using section number and question number, S2 Q1 representing Section 2 Question 1.

### *2.3 Actual Password Practice*

In this section the survey aimed at establishing the actual password behavior of the respondents. A Likert Scale

| Questions | Question Description |
|---|---|
| S1Q1 | What is your gender? |
| S1Q2 | Are you a student or a staff? |
| S1Q3 | What is your course of study or what department do you work with? |
| S1Q4 | What device(s) do you employ the use of passwords? |
| S1Q5 | What online service(s)/account(s) do you have that requires the use of passwords on? |

Table 1. Demographics

| Questions | Question Description |
|---|---|
| S2Q1 | Have you received guidance on password creation in the past? |
| S2Q2 | If "Yes" Where or from Whom? |
| S2Q3 | What do you feel should be the minimum character length of a password? |
| S2Q4 | What do you feel a password should be made up of? |
| S2Q5 | Do you feel a password should contain symbols? for example @ ! $ < # _ & % etc |
| S2Q6 | How frequently do you feel users should change their passwords? |
| S2Q7 | Do you feel users should delete their online accounts when they are no longer in use? |
| S2Q8 | Should users write down their passwords on notes, in text files, etc.? |
| S2Q9 | Briefly describe what a good password should contain |

Table 2. Theoretical Password Policy Knowledge Questions

ranging from 1 to 5 was used for certain questions as shown in Table 3, where 1 stood for "always", 2 stood for "yes", 3 stood for "sometimes", 4 stood for "no" and 5 stood for "never". The questions in Table 3 are labelled using section number and question number, S3Q1 representing Section 3 Question 1.

### 3. Survey and Findings

This section reports on the results and findings of the survey. The respondents consisted mainly of students and staff under IT inclined departments; however other interested members from other departments who showed interest were allowed to participate. Students who participated ranged from 100 level students (1st year) to postgraduate students.

The survey captured a total of 481 respondents. It comprised of 72 (15%) 100 level students, 79 (16.4%) 200 level students, 70 (14.6%) 300 level students, 89 (18.5%) 400 level students, 96 (20%) 500 level students, 18 (3.7%) Postgraduate Student and 57 (11.9%) Staff.

#### *3.1 Theoretical Password Knowledge*

Section 2.2 of the questionnaire aimed at establishing the theoretical knowledge of respondents with regard to passwords policies. Table 4 summarizes responses to the questions asked in this section.

| Questions | Question Description |
|---|---|
| S3Q1 | Do you reuse old password you had earlier used? |
| S3Q2 | Do your passwords only contain plain text with no special symbols such as numeric and alphanumeric characters? |
| S3Q3 | Are your password lengths less than 10 characters? |
| S3Q4 | Have you ever used the same password across multiple accounts/device(s)? |
| S3Q5 | Have you ever used `12345` or `password` for a password? |
| S3Q6 | Have you ever used family member names, usernames and personal dates as passwords? |
| S3Q7 | Have you ever used dictionary words as passwords? |
| S3Q8 | How often do you change your passwords? |
| S3Q9 | Which of the following statements is best suited to describe how you remember your passwords? |
| S3Q10 | Do you write your passwords down? |
| S3Q11 | If "Yes" where do you write your passwords down? |
| S3Q12 | Do you share your passwords? |
| S3Q12 | If "Yes", who do you share them with? |
| S3Q14 | Do you delete your online accounts if you have not used them for a long time? |
| S3Q15 | Do you reuse your regular passwords on accounts/services that you think should be extra protected? |

Table 3. Actual Password Practice Questions

For S2Q1, 352 (73.2%) of the respondents stated having received guidance on creating passwords. For S2Q5, 295 (61.3%) of the respondents were of the opinion that passwords should contain symbols, whereas 162 (33.7%) respondents said "No" and 24 (5%) respondents stated that they did not know. For S2Q7, 376 (78.2%) respondents were of the opinion that online accounts should be deleted if not being used, whereas 88 (18.3%) stated they should not. For S2Q8, 275 (57.2%) respondents were of the opinion that passwords should not be written down, whereas 191 (39.7%) respondents stated users should write down their passwords and 15 (3.1%) respondents stated that they did not know. Table 5 summarizes responses from other theoretical password knowledge questions the survey asked.

As shown in Table 5, for S2Q2, 109 (27.9%) respondents stated they received password guidance while studying, 174 (44.6%) from websites or newspapers and 49 (12.6%) received guidance from friends.

For S2Q3, 163(33.9%) respondents were of the opinion that the minimum number of characters should be six, 29

| Questions | Yes | No | I Don't Know |
|---|---|---|---|
| S2Q1 | 352 (73.2%) | 90 (18.7%) | 39 (8.1%) |
| S2Q5 | 295 (61.3%) | 162 (33.7%) | 24 (5%) |
| S2Q7 | 376 (78.2%) | 88 (18.3%) | 17 (3.5%) |
| S2Q8 | 191 (39.7%) | 275 (57.2%) | 15 (3.1%) |

Table 4. Theoretical Options N=481

| Questions | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 |
|---|---|---|---|---|---|
| S2Q2 | While Studying | Websites/ Newspaper | From Friends | Other | |
| | 109 (27.9%) | 174 (44.6%) | 49 (12.6%) | 58 (14.9%) | |
| S2Q3 | 6 | 7 | 8 | 9 | 10 |
| | 163 (33.9%) | 29 (6%) | 237 (49.3%) | 11 (2.3%) | 41 (8.5%) |
| S2Q4 | Uppercase Letters | Lowercase Letters | Combination of both | Don't Know | |
| | 3 (0.6%) | 26 (5.4%) | 443 (92.1%) | 9 (1.9%) | |
| S2Q5 | Every 90 days | Every 120 days | Never | Don't Know | |
| | 220 (45.7%) | 64 (13.3%) | 92 (19.1%) | 105 (21.8%) | |

Table 5. Theoretical Questions Results N=481

(6%) that the minimum number of characters should be seven, 237 (49.3%) that the minimum number of characters be eight, 11(2.3%) that the minimum number of characters should be nine and 41 (8.5%), that the minimum number of characters should be 10.

For S2Q4, 3 (0.6%) respondents felt a password should be made up of upper case letters, 26 (5.4%) respondents felt a password should be made up of lower case, 443 (92.1%) respondents felt a password should be made up of combination of both and 9 (1.9%) respondents did not know what passwords should be made up of.

For S2Q6, 220 (45.7%) respondents felt a password should be changed every 90 days, 64 (13.3%), respondents felt a password should be changed every 120 days, 92 (19.1%) respondents felt a password should never be changed and105 (21.8%) did not know if password should be changed. For the open-ended question, S2Q9, most of the respondents indicated that a password should contain a combination of uppercase and lowercase characters, numbers and special characters. Based on these results, it is clear that the respondents are equipped with the necessary theoretical knowledge with regard to good password management.

### *3.2 Actual Password Practice*

This section discusses the results and findings relating to the actual password practice of students and staff. Table 6 lists the questions which were asked using a 5-point Likert Scale where 1 = "always", 2 = "yes", 3 = "sometimes", 4 = "no", and 5 = "never". Questions not using the 5-point Likert Scale are left out from this table and discussed later.

Table 6 shows the average for the questions asked in section 2.3. It made use of a 5-point Likert Scale response option. In the Table 6, an average of higher or equal to 4.0 indicates good password practice. However as can be observed all fall (Average of S3Q1, S3Q2, S3Q3, S3Q6, S3Q7, S3Q15) below 4.0 (that 2.70, 3.43, 2.73, 3.14, 3.82, 2.73 respectively). Therefore, no good password practice was observed across the respondents. Questions with an average of less than 3.0 indicate fairly poor practice. From Table 6 it can be observed that the respondents had poor practice when it comes to reuse of old password

| Questions | Scale | | | | | Total | Average |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | | |
| S3Q1 | 69 (69) | 133 (266) | 175 (525) | 60 (240) | 40 (200) | 1300 | 2.70 |
| S3Q2 | 34 (34) | 66 (132) | 94 (282) | 186 (744) | 92 (460) | 1652 | 3.43 |
| S3Q3 | 57 (57) | 157 (314) | 136 (408) | 82 (328) | 42 (210) | 1317 | 2.73 |
| S3Q6 | 44 (44) | 148 (296) | 62 (186) | 109 (436) | 110 (550) | 1512 | 3.14 |
| S3Q7 | 20 (20) | 55 (110) | 46 (138) | 173 (692) | 176 (880) | 1840 | 3.82 |
| S3Q15 | 73 (73) | 149 (298) | 95 (285) | 94 (376) | 57 (285) | 1317 | 2.73 |

Table 6. Likert Scale Questions N=481

they had earlier used, their password lengths were less than 10 characters and indulge in the use of regular passwords to protect those accounts which require extra protection.

For S3Q1, 69 (14.5%) respondents stated they "always" reuse their password whereas 40 (8.4%) respondents stated they "never" reuse their passwords. For S3Q2, only 92 (19.5%) respondents said their passwords were "never" plaintext only, whereas 34 (7.2%) respondents passwords were "always" plaintext. For S3Q3, 57 (12%) respondents stated that their passwords were "always" less than 10 characters, 136 (28.7%) respondents indicated "sometimes". For S3Q6, only 110 (23.3%) respondents stated that they "never" use personal dates and family member names as passwords. For S3Q7, only 176 (37.4%) respondents said they "never" use dictionary words as passwords, and for S3Q15, only 57 (12.2%) respondents stated that they "never" use their regular password in the accounts they think should be extra protected.

For S3Q4, 378 (79.7%) respondents have used the same password for multiple accounts. Similarly, for S3Q5, 362 (76.1%) respondents said "No" to this question. This is a good sign and shows that a large number of people do not use such simple passwords. For S3Q8, 40 (8.4%) respondents indicated that they change their passwords every 120 days and 148 (31.2%) respondents do not change their passwords. For S3Q8, 121 (25.5%) respondents change their passwords every 90 days. For

S3Q12, 332 (70.9%) respondents do not share passwords. For S3Q14, 276 (58.7%) respondents do not delete their online accounts if they have not used them in a long time.

### 4. Discussion of the Survey Results

This section discusses the results and findings from the survey and compares the theoretical password knowledge with the actual password practice of respondents. There are a number of theoretical password knowledge questions, as were seen in Table 2, which can be correlated to the actual password practice questions, as seen in Table 3. Table 7 lists the theoretical and practice related questions that can be correlated.

Figure 1 represents the respondents' theoretical password knowledge compared to their actual password management practice. For these results, only the top most answered questions are represented.

As can be observed in Figure 1, there is a significant difference between the respondent's theoretical password knowledge and their actual password practice.

In S2Q3 and S3Q3, which referred to the minimum password length, it can be observed that the respondents know what the minimum average length should be for a password but when it comes to actual practice they do not adhere to what they know.

| Characteristic | Theoretical Password Knowledge Questions | Actual Password Behavior Questions |
|---|---|---|
| Password characteristics | S2Q4 | S3Q2 |
| Changing passwords | S2Q6 | S3Q8 |
| Delete online accounts | S2Q7 | S3Q14 |
| Writing passwords down | S2Q8 | S3Q10 |

Table 7. Correlation Between Theoretical Password Knowledge Question and Actual Password Practice Questions

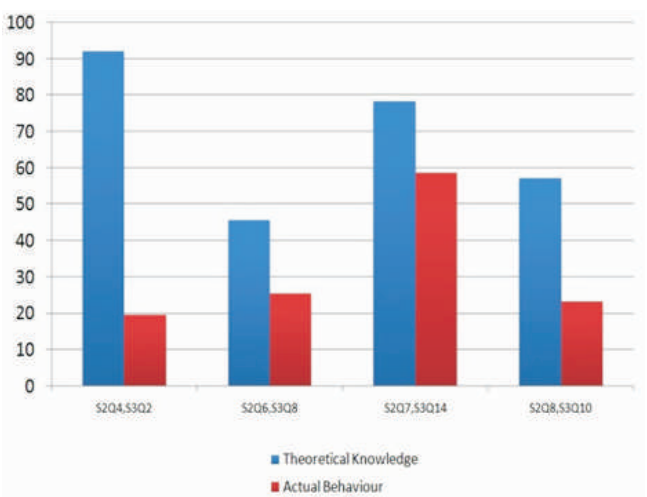


Figure 1. Theoretical Password Knowledge Versus Actual Password Practice of Respondents

When asked what passwords should be made up of in S2Q4, 443 (92.1%) of the respondents were of the opinion passwords should be made up of a combination of upper case and lower case letters. This implies they are well aware of the policies that strong passwords should be complex (combination of upper, lower, special characters). However, when asked if their passwords only contain plain text with no special symbols such as numeric and alphanumeric characters in S3Q2, only 92 (19.5%) said never. This implies when it comes to actual practice, only less than 20% of the respondents adhere to the policy. This was in contrast to 92.1% of who know strong passwords should be a combination.

When asked how frequently they feel the passwords should be changed in S2Q6, 220 (45.7%) of the respondents were of the view that passwords be changed at least every 90 days. However, when asked how often they change their passwords in S3Q8, only 121 (25.5%) said they do every 90 days. On the other hand, 148 (31.2%), (almost as much as those that do every 90 days) said they never change their passwords and 166 (34.9%) do not even know if passwords should be changed. Thus, only a few frequently change their passwords in practice.

When asked if they feel account users should delete their online accounts when they are no longer in use in S2Q7, 376 (78.2%) of the respondents were of the opinion that online accounts should be deleted when they are no longer in use. However, when asked if they delete their online accounts they have not used for a long time in S3Q14, 276 (58.7%) said they do not. This implies it makes sense to them that online accounts no longer in use be deleted, yet over half the sample respondents do not use this theoretical knowledge in practice.

When asked in S2Q8 if users should write down their passwords on notes or in text files, 275 (57.2%) said they do write down their passwords on notes or in text files. However, 110 (23.2%) admitted to writing down

passwords and another 111 (23.4%) admitted to doing so sometimes. This implies although over 57% know it is bad practice to write down their passwords, close to half the sample population still write down passwords.

When asked in S3Q4 if they use the same password across multiple accounts/device(s), 378 (79.7%) said yes regardless of the obvious down sides of doing so. As discussed earlier they know what a strong password should look like yet rather find it more convenient using the same password across multiple accounts, devices and services. This is even more an issue as was established by S3Q15 when asked, "Do you reuse your regular passwords on accounts/services you think should be extra protected?" 73 (15.6%) admitted they always reuse regular passwords on such accounts, 149 (31.8%) said Yes and 95 (20.3%) admitted they sometimes reuse regular passwords on accounts/services they know should be extra protected.

## Conclusion

User authentication is one of the most important security characteristics of any system given today's globalized digital life style. The safety and security of not only sensitive data, privacy but also critical infrastructure relies primarily on authentication. Amongst all authentication schemes, text-based passwords are mostly deployed across various platforms thus the importance of evaluating user password management practice cannot be overemphasized. Following the theoretical password knowledge findings and results from the survey conducted, it can be observed that the target respondents are knowledgeable on good password management policies. However, actual password practice results show they do not comply and effectively implement the theoretical password knowledge they possess. Thus it can be concluded that there is a significant difference between what respondents know compared to their actual practice. Numerous implications abound when this is the case as it makes users more vulnerable to security risks of unauthorized access by unauthorized users. This research survey was limited to students and staff of the Federal University of Technology, Minna with emphasis on Information Technology inclined departments. The results are not to be generalized but are however consistent with that of a study conducted by (Fredericks, Futcher, & Thomson, 2016) in South Africa.

## Recommendations

There clearly exists no "short cuts" to ensuring user safety and security as it concerns authentication. From the research findings, text based password pose a memorability problem that will continuously compel user to employ unsecured means of handling passwords. The need on that note, for an alternative to text passwords cannot be overemphasized. Graphical passwords are a relatively new scheme that tackles the memorability problem faced by the text based scheme. This is because users can remember images more easily than text.

## Despite the Advantages

Graphical passwords are yet to be widely deployed for online products and services. This may be because the proposed Graphical passwords only provide theoretical entropies between 12 and 23 bits which are far from the 39 to 53 bits offered by the text-based schemes. The authors recommend further and more extensive research into enhancing graphical password entropies as they possess the potential to replace text passwords.

## References

**[1]. Blanchard, J. (2014).** Weak passwords put millions at risk of bank accounts and other information being hacked online. *Mirror.* Retrieved from http://www.mirror.co.uk/news/technologyscience/technology/weak-passwords-put-millionsrisk-4439460

**[2]. Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., & Biddle, R. (2009, November).** Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (pp. 500-511). ACM.

**[3]. De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005).** Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies,* 63(1-2), 128-152.

**[4]. Florêncio, D., Herley, C., & Van Oorschot, P. C (2014).** An administrator's guide to internet password research. In *Proceedings of the 28th USENIX Large Installation System Administration Conference* (pp. 35-52).

**[5]. Fredericks, D. T., Futcher, L. A., & Thomson, K. L. (2016).** Comparing Student Password Knowledge and behavior: A case Study. In *Proceedings of the Tenth International Symposium on Human Aspects of Information and Assurance (HAISA 2016)* (pp. 167-178).

**[6]. Helkala, K., & Bakås, T. H. (2014).** Extended results of Norwegian password security survey. *Information Management & Computer Security,* 22(4), 346-357.

**[7]. Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., ... & Cranor, L. F. (2013, April).** The impact of length and mathematical operators on the usability and security of system-assigned one-time PINs. In *International Conference on Financial Cryptography and Data Security* (pp. 34-51). Springer, Berlin, Heidelberg.

**[8]. McDowell, M., Rafail, J., & Hernan, J. (2009).** Choosing and protecting passwords. *US-CERT Cyber Security Tip ST04-002.* Retrieved from https://www.us-cert.gov/ncas/tips/ST04-002

**[9]. Microsoft (2013).** *Maximum password age.* Retrieved from https://technet.microsoft.com/enus/library/hh994573(v=ws.10).aspx

**[10]. Notoatmodjo, G. (2007).** *Exploring the 'weakest link': A study of personal password security* (Doctoral Dissertation, University of Auckland).

**[11]. Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. (2013, September).** Are graphical authentication mechanisms as strong as passwords? In *Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on* (pp. 837-844). IEEE.

**[12]. Ritó, E. (2018).** Smart Cities for a better world. *Central European Publications,* 2(41), 42-53.

**[13]. Stobert, E., & Biddle, R. (2014).** The password life cycle: User behaviour in managing passwords. In *Symposium on Usable Privacy and Security (SOUPS), Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance* (pp. 243-255).

**[14]. Slain, M (2016).** Announcing Our Worst Passwords of 2015. In *TeamsID.* Retrieved from http://www.teamsid.com/worst-passwords-2015

**[15]. University of Illinois (2014).** Why you should use different passwords. University of Illinois. Retrieved from https://security.illinois.edu/content/why-you-should-use-different-passwords

## ABOUT THE AUTHORS

*Victor N. Adama is a Lecturer in the Department of Computer Science at Federal University of Technology, Minna. He is currently pursuing Ph.D in Computer Science. His research areas of interest are Security and Human Computer Interaction.*

*Noel Moses Dogonyaro is a Lecturer in the Department of Cyber Security Science at Federal University of Technology, Minna. He is currently pursuing Ph.D in Cyber Security Science at the same University. His major areas of research include: Cryptography, Block Chain Technology, Information Security, Network Security and Data Mining.*

*Victor L. Yisa is a Lecturer in the Department of Cyber Security Science at Federal University of Technology, Minna. He is currently pursuing Ph.D in Computer Science. His major Research areas of interest are in Social Engineering, Cyber Self Defence and Network Security.*

*Baba Meshach is a Lecturer in the Department of Cyber Security Science at Federal University of Technology, Minna. His major research areas of interest are in Security Intelligence for Trending Events, Dependency Visualization and Network Security.*

*Ekundayo Ayobami is a Lecturer in the Department of Computer Science at Federal University of Technology, Minna. Her areas of interest are Data Mining, Artificial Intelligence and Human Computer Interaction.*

i-manager®
Publications

3/343, Hill view, Town Railway Nager, Nagercoil
Kanyakumari Dist. Pin-629 001.
Tel: +91-4652-276675, 277675

e-mail: info@imanagerpublications.com
contact@imanagerpublications.com
www.imanagerpublications.com

i-manager Printing Press