BOOK CHAPTER | Password Habits

Password Habits & Management Practices Amongst Millennials Driving Cybersecurity Trends

Talabi, A.A., Longe, O.B., Muhammad, A.A. & Olusanya, K.
Doctoral Programme in Cyber Security
African Centre of Excellence in Technology Enhanced Learning
National Open University of Nigeria, Abuja, Nigeria
E-mails: doyin.talabi@gmail.com; Olumide.longe@acity.edu.gh; muhdaminu@kasu.edu.ng; kunlesanya2002@gmail.com

Abstract

Many computer users have multiple online accounts and passwords for different applications and websites. These accounts are used for communication, collaboration, social networking and financial transactions via different platforms and devices. This sometimes makes users to be negligent in password creation and create weak or easy-to-guess passwords, re-use the same passwords, making their accounts vulnerable to compromise and theft with dire consequences. The goal of the paper was to research password creation habits and management practices, among millennials who are known to be active online and obsessed with mobile devices and social media networks like Facebook and Twitter. The survey method was used and a structured questionnaire was designed and circulated among 110 young undergraduates in three higher institutions in Yaba Area of Lagos, Nigeria. The findings from the project revealed that while respondents, many of them millennials, recognize that computer security is important, their habits run contrary to their knowledge as they choose convenience over security. Millennials are comfortable with technology, but have poor password management practices and rely on in-built security in applications. Many reuse same passwords for multiple online accounts and use password management apps to help them remember passwords. The study also shows that Millennials are more likely to adopt biometrics, multi-factor authentication and other passwordless methods than the older generation. The number of millennials in the workplace is growing and as a result they may shape the future of cybersecurity practices away from classic passwords to other more convenient but secure authentication techniques.

Keywords: Authentication, Cybersecurity, Habits, Internet, Millennials, Passwords, Passwordless,

Introduction

According to Internet world statistics website, internetworldstats [1] , out of a world population estimated at 7.8 Billion people as at end of March 2021, internet users are estimated at 5.16 billion people (about 65.6%). This means that real–time communication and collaboration is available to millions of people through multiple devices and channels around the world.

Citation Talabi, A.A., Longe, O.B., Muhammad, A.A. & Olusanya, K. (2022). Password Habits & Management Practices Amongst Millennials Driving Cybersecurity Trends. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series Book Chapter on Web of Deceit - African Multistakeholders' Perspective on Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical and Design Approaches. Pp 173 -178. www.isteams.net/bookchapter2022. DOI https://doi.org/ 10.22624/AIMS/BK2022-P29

Thus, the internet has provided a cheap and effective means of communication and collaboration among different people, groups and organizations in different places around the world in real time in a global village where geographical distances have become blurred. With the exponential growth in the use of computers, mobile devices, social networking and computer-based systems, resulting in millions of devices connected together globally, information privacy and confidentiality has become a major issue.

Data has become a strategic resource and adequate security must be in place to protect individual, corporate and national data from unauthorized access, theft, loss, or even crash of information systems infrastructure resulting in break down or stoppage of operations, loss or reputation or systems shut down. The issues around confidentiality, integrity and availability of data and systems have become critical. There has been an increase in data privacy breaches and break-ins resulting in the theft and loss of data at personal, organizational and national levels, damage to systems and collapse of entities. This paper attempts to research password creation and management practices by users of the internet, especially the millennials

Related Works

According to Steve Harris (2018) [2] , the theme on poor password security has been on for a long time, in spite of repeated warnings from IT professionals on the consequences of malicious attacks on user accounts. A report from Preempt found that 35 % of users have weak passwords and other 65% can be cracked. In 2017, The Ponemon Institute discovered that 35% of companies surveyed have but do not enforce their password policy. An IBM Survey found that 67% of users are comfortable using biometric authentication while about 75% of millennials are at home using biometrics. 50% use complex passwords, and 41% admit to reusing old passwords. The time to replace passwords with biometrics has come. Many users manage more than 150 online accounts and biometrics can provide better security and more convenience and millennials preference for biometrics may affect workplace practices and enterprises will need to adapt. We may no longer have to remember multiple passwords and we log in with our face, hands, voices and even eyes.

The Digital Guardian (Nate Lord) (2017) [3] surveyed 1,000 Google randomly selected users in the United States, aged 18 and above on their password habits. The survey found that many people are suffering from password overload, due to the numerous online accounts and multiple passwords to remember. 29% of the respondents have too many accounts and are not sure of how many accounts require password. 29.7% of respondents have less than 10% of their accounts requiring passwords, 13.6 % have more than 25 accounts that require a password and 27.6% have between 11 and 25 accounts requiring password. It also found that users update their passwords frequently and 31.3% of respondents change their passwords two times a year, 22.4% change their passwords more than five times per year, and 17% change their passwords approximately three to four times a year and about 29.4% say they never change their passwords.

The survey indicated that 49.3% only re-use passwords for unimportant accounts, 39.9% never re-use passwords and 10.8% have only one default password that they use for almost all their accounts. The survey also found that 55.8% use complex passwords, 37.8% use fairly complex passwords and 6.5% use common words like pet names, children as passwords. According to the survey, 65.3% of respondents consider security as the most important factor in selecting unique and complex passwords, while 34.7% place more importance on using passwords that are easy to remember. 32.8% of respondents do not know what two-factor authentication is, 47.8% will use it where available and 19.4% do not.

Two-factor authentication involves using two distinct criteria to verify a user's identity; this is usually a combination of something you know (e.g., your password or your username), something you have (e.g., your ATM card, mobile phone, or an access token/badge) and something you are (biometric features, like fingerprint or iris.). Brain Krebs says since most websites will email any forgotten password back to the user, the most secure method for remembering passwords may be to have a list of login names and clues for each every Web site for which you have a password. The survey concluded that more education on password hygiene and practices are needed, as we depend more on digital systems to live.

According to a publication by New York University [4], passwords have always been an issue, because they are expensive, inconvenient and insecure. Passwords alone are responsible for majority of data breaches and cyberattacks. Due to the fact that a user can generate and store a minimal number of complex words, many end up with bas password habits of storing passwords in an unsecured computer document, writing it down or reusing the same password and thereby increases the chances of successful cyberattack. Millennials grew up with and are expected to be conversant with technology and cybersecurity practices.

However, studies have shown that some millennials may not be fully aware of the security threats they face and still have different online and information security behaviour despite these awareness and still engage in risky behaviour that can compromise their security. Many Millennials have not adopted the use of password managers despite their growing popularity as only 31% use a password management app and many use public Wi-Fi because of convenience, despite the possibility of compromising their personal security while connected. The report concluded that password managers, biometrics, and multi-factor authentication will replace traditional methods like passwords and millennials will play a large role in making this a reality.

Munyard (2018) [5] says that though password has been maligned for years, it is still the most used for access and identity protection. Despite years of educating people to use difficult-to guess passwords, many still use simple passwords like '123456'. From studies by IBM, millennials may lead the breaking of our addiction to passwords. The study found that 42% of millennials use complex passwords containing combinations of different characters and symbols as opposed to 49% for people over 55 years old. Typically, Generation Z, those born between 1998 and 2017 use 5 passwords regularly, millennials, those born between 1981 and 1997 use 8 passwords regularly and older generations use 12 passwords regularly. The study also found that younger people are willing to trade convenience and time for security Nevertheless, Generation Z use digital password managers and are actually more careful to store and secure and store digital credentials as compared to other age groups and are more open to using two-factor authentication and biometrics as secondary levels of protection.

Fewer young people have multiple debit/credit cards, mortgages, stocks and have less to protect but surprisingly and may not guard their online accounts aggressively, but because are comfortable with technology , they are early adopters of biometrics and newer forms of protection because they mostly access the internet from mobile devices . Millennials seem to be the one that will remove our reliance on passwords and even teach elders, some new things due to their disposition to using new technologies. According to [6] Millennials are sometimes accused of disregarding security but they are early adopters of passwordless authentication and comfortable with biometrics. Some will use password managers, and let the app create and manage complex passwords for them so that they do not have to remember them all. Many may not agree, but Misan Etchie (2021)[7] says the older generation are not as knowledgeable as millennials, who are comfortable and tech- savvy are digital natives, having grown up with technology. Ageism, as this is called, may be the cause for age stereotypes and generation-based biases as regards technology usage. It is common to see millennials adapt to using an app or device, just a few hours after handling it, (a source of worry for young mothers about addiction to mobile devices by children) and many older relatives rely on their young ones to help with using web services and accessing online financial services.

However, though millennials are more knowledgeable about technology, they are more likely to engage in risky online behaviour like sharing online credentials with others, which can compromise their online security and confirmed by a study that about 23% of millennials did so. These dissimilarity in password habits and privacy approaches by different generations may affect enterprise security practices as millennials are becoming the largest demographic group in the workplace. Also, older adults may have be learn to adopt newer authentication methods other than passwords and this might lead to a wide adoption of biometrics, multi-factor authentication and passwordless technology in the near future.

Though the complacent attitudes of many young people towards good cybersecurity practices may look bad from the surface and password habits are getting worse, these might just hint at a future with more convenient and more secure authentication technology – a future where the traditional password is replaced by multi-factor authentication, biometrics and passwordless technology. Millennials are conversant with unlocking their mobile devices with fingerprint and face recognition software and this may be why they choose convenience over security. Visual Objects [8] surveyed 500 full time employees to find out how behaviour about cybersecurity affects enterprise success with cyber defense. The survey found that 91% of employees felt that the organization is responsible to handle cybersecurity issues not the workers. 63% have used the same passwords for multiple online accounts at work and on devices. 63% of employees are comfortable with storing personal information on work devices despite attendant risks. 27% of the older generation more susceptible to attacks because of no concern about where they store personal data. Older generation follow more reliable protection practices than younger people and only 2% of them reuse work-related passwords as compared to 13% of millennials who always reuse passwords. Only 17% of millennials are not concerned about storing passwords on work devices.

The older generation are vulnerable to scams due to poor awareness and struggle with breaking the habit of mixing work and personal data on same devices, something less common with millennials. Passwords saved on devices are potential sources of data breach. Due to the uptake of remote work, organizations must ensure use of strong and different passwords on work devices. Cybersecurity experts recommend using central password managers, automatic reset of passwords after a defined interval and two-factor authentication.

Millennials grew up with technology and have poor password practices because they trust that online services come with built-in security and have their best interest in mind. However, the older generations lack the technical comfort to trust built-in security measures and this suspicion about password safety make tem proactive in protecting their accounts. Employees must be at the forefront of workplace cybersecurity measures and organizations must recognize their role in securing corporate data and develop a strong cybersecurity culture with buy-in from all employees. In addition, organizations should invest in security training and education, test understanding of the cybersecurity practices after training, build a solid foundation for data governance and control, and equip staff with tools and software required for implementation and compliance

Methodology

Research Design -The Research Design adopted for this study is the survey design. A survey research according to Nworgu (1991) [9] is one which a group of people or items is studied by collecting and analyzing data from only a few people or items considered to be representative of the entire group. The population for the study was 110 young undergraduate students of the University of Lagos, Federal College of Education (Technical), Akoka and the Yaba College of Technology, all in the Mainland Area of Lagos. The objective of this research paper is to analyze the password creation patterns and password management methods and practices among millennials as compared to the older generation

Results

The findings from the study indicated that majority of the respondents are young people between the ages of 16 and 35. Majority of the respondents are undergraduates and ordinary users of computers and mobile devices. Majority of the respondents access the internet through their mobile phones. Majority of the respondents opened their e-mail accounts between 2006 and 2015 and very few before Year 2000.

Majority of the respondents considered computer security as an important issue. The survey showed that about 10% of the respondents had passwords with less than six characters, while majority had passwords with between six and ten characters and a minority had passwords with over twelve characters. Majority of the respondents always use a mix of different characters when creating passwords and a minority use mixed characters when the systems forces them to do so. Majority of respondents have between two and five online accounts, with a minority having over fifty online accounts. Majority of respondents use their online accounts daily, which indicates the importance of their accounts to their daily activities.

Majority of respondents store passwords in their heads and very few store passwords in notebooks or use password managers and apps. More than half of respondents use same passwords for multiple accounts and websites and a third use the same passwords for multiple accounts and websites. Few of the respondents change their passwords either monthly or every six months, which mean they are susceptible to unauthorized access or their online accounts compromised. Many of the respondents rarely change their passwords or only when forced to do so. This suggests that while they recognize that computer security is an issue, yet their behavior suggests otherwise.

About a third of respondents share their passwords either by oral communication, telephone or by writing on paper. Majority had never had never had their personal information stolen, Many had never had their online passwords compromised and only about a third of respondents had been tricked online to reveal their PIN/Passwords and majority are satisfied with their current password management habits. Majority of the respondents have multiple online accounts with more than half of respondents using same passwords for multiple accounts and about a third have been tricked into revealing their PIN/Passwords. Many respondents recognize are satisfied with their current passwords management habits, but the habits are not best practice and expose their online accounts to compromise, hacking and theft.

Conclusion

The survey revealed that while respondents recognize that computer security is an important issue, their actions run contrary to their password management habits and the expected outcome of their habits. These results show that while respondents want secured passwords for their online accounts, their actions put their accounts at risk. This confirm studies that show that millennials have poor password management habits. Many reuse same passwords for multiple accounts and rarely change passwords, except when forced to do so. These habits clearly expose online accounts to risk of compromise and theft.

The survey confirmed studies highlighted in the literature review that many millennials have poor password management habits and cybersecurity practices and prefer convenience over security. The studies further confirm that this is because millennials are comfortable with technology, they rely on built-in security controls and trust that the password management applications would remind them of their passwords if they forget them. The studies also confirm that millennials are more likely to adopt biometrics, multi-factor authentication and other passwordless methods, which they are already doing on their mobile devices. Therefore, because millennials are many in the workplace, they will likely shape the future of enterprise and industry cybersecurity practices away from classic dependence on passwords to more secure authentication systems.

The recommendations is that organizations should invest in cybersecurity training and education to build a strong cybersecurity culture with employee buy-in , undertake security drills regularly, and have data governance policies in place for management and control of sensitive data like passwords. This should minimize exposure to risk and compromise and use a platform for secure password management habits and practices.

References

[1] Miniwatts Marketing Group. Internet Usage and World Population Statistics estimates. (2021) www.internetworldstats.com. (Accessed 12/01/2022)

[2] www.orange-business.com . Harris Steve (2018). Password-what password. Millennials are moving security on. https://www.orange-business.com/en/blogs/password-what-password-millennials-are-moving-security 09/01/1022 (Accessed 09/01/2022)

[3] www.business-standard.com. Nate Lord (2017). Digital Guardian. Password hygiene for cybersecurity: millennials driving a positive change.https://www.business-standard.com/article/current-affairs/password-hygiene-for-cyber-security-millennials-driving-a-positive-change-117062001226_1.html Accessed 09/01/2022

[4] www.nuy.edu. eleven40 Pro on Genesis Framework (2022). Millennials and Cybersecurity: Passwordless Future Fast Approaching. https://wp.nyu.edu/dispatch/millennials-and-cybersecurity-passwordless-future-fast-approaching/ Accessed 09/01/22

[5] www.securityintelligence.com. Michael Bunyard. March 5, 2018. Young People May Shun Passwords, But That Doesn't Mean They're Less Identity-Conscious. https://securityintelligence.com/young-people-may-shun-passwords-but-that-doesnt-mean-theyre-less-identity-conscious/ . Accessed 09/01/22

[6] . www.techrepublic.com. Limor Kessem (2018). Millennials are moving beyond the password. https://www.techrepublic.com/article/ibm-security-report-millennials-are-moving-beyond-the-password/ accessed 09/01/22

[7] www.infosecurity-magazine.com. Misan etchie. (2021). Password habits differ generations. https://www.infosecurity-magazine.com/next-gen-infosec/password-habits-differ-generations/ Accessed 0n 10/1/2022

[8] Visualobjects.com Sydney Wess. 2020. Employees & Cyber Defense. https://visualobjects.com/app-development/blog/cybersecurity-topics-cyber-defense. Accessed 11/1/2022

[9] Nworgu, B.G. (1991). Educational Research: Basic Issues & Methodology. Ibadan: Wisdom Publishers .Accessed 13/1//2022