IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 10, October 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

A Review on the Strategies of Password

Yogesh S. Sakhare, Poonam R. Parihar, Neha D. Borle, Nikita D. Borle

Students, Department of Information Technology, Anuradha Engineering College, Chikhli, India

ABSTRACT: Research has shown that password security practices typically conflict with general usability principles. Though the challenges faced by low-
literacy users when creating and managing passwords are likely to extend beyond those experienced by the general pu blic, little research has been done to explore password usability in this at-risk group. This survey of 20 low-
literacy participants aims to examine password behaviors within this population, including password creation, recall st rategies, and perceptions of password strength and security. It expands on the work of Chisnell and Newby (2015) bas ed on a nationwide survey exploring password use, password creation strategies, and perceptions regarding password s ecurity. Thus, this study allows for comparison between password use and perceptions among the broader population a nd those of users with low literacy skills. These results provide important insights into patterns of use and mental mod els of password requirements and password security among low-
literacy users. Keywords Password security, usability, low literacy

GENERAL TERMS

password management, user behavior, password reuse

KEYWORDS

security, password, survey, user behavior

I. INTRODUCTION

For years, research has shown that password security practices strongly conflict with general usability principles. Ofte n, security measures such as password composition policies seek to increase a user's password strength without consid ering the goals or cognitive ability of the user (Weirich & Sasse, 2001). Working memory limitations, memory decay due to infrequent use, and difficulty recalling non-
meaningful passwords all make the process of creating and recalling passwords a significant cognitive burden. This pr ocess is made even more difficult by the proliferation of passwords in daily life, from bank pins to device passwords a nd account credentials. In order to meet the cognitive demands of password use, individuals often rely on strategies th at increase password memorability at the cost of reducing password strength and security. These strategies were recent ly explored by a national survey funded by the National Institute of Standards and Technology asking 300 respondents to describe their password use, their strategies for creating passwords, and their perceptions regarding password secur ity (Chisnell & Newby, 2015). The challenges relating to password usability weigh even more heavily on the nearly h alf of the U.S. population that reads at Basic or Below Basic levels as measured by the National Adult Literacy Surve y (Kutner, 2007). Limited vocabulary, low computer literacy, and difficulty typing and spelling already put such users at a disadvantage when using the web (Zarcadoolas, Blanco, Boyer, & Pleasant, 2002). Internet users with low literacy skills face challenges in navigating, searching, and reading information online (Birru et al., 2004; Birru & Steinman, 2004; Kodagoda & Wong, 2008; Summers & Summers, 2005). They face particular difficulties in navigating forms on line—
including challenges in creating usernames and passwords (Summers et al., 2006). For these internet users, the strain c aused by password usability issues adds to their existing cognitive burden. Despite this increased challenge, little resea rch has been done to explore password usability in this at-
risk group. The current survey of 20 low literacy participants aims to examine password behaviors within this populati on, including password creation, recall strategies, and perceptions of password strength and security. It expands on the work of Chisnell and Newby, allowing for some comparison between the password creation strategies and perception s around password security across the broader population and those with low literacy skills.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

1.1User ID and Password

First, users are either assigned an ID or are given the chance to create one. Once the ID has been created, the user cho oses a password. The password should be secret and shared only between the user and the information systems or com puter. Users should not disclose their passwords or write them down.

1.2 Log-on

During the login process, users must enter both their user IDs and passwords. The system then processes and compare s the ID and password with what is stored in the database. If the user ID and password match, the user will be granted access to the system. If the user ID and password do not match, the user will not be allowed access. Many information systems suspend a user account after three to five unsuccessful login attempts. The users must then visit a system ad ministrator to reset the password. Since 1970, instead of storing all passwords in a file, passwords have been stored in a cryptographic hash (Schneier, 2000). When the user types her password into a computer, website, or software applic ation, the software calculates the hash of the password and compares it with the hash stored in the file (Schneier, 2000). If they match, the user is allowed in (Schneier, 2000). However, if a cracker has acquired a copy of the hashed pass word file, the cracker can use a dictionary to compute the hash of every word in the dictionary (Schneier, 2000). If the hash word matches a password entry, then the cracker obtains a password (Schneier, 2000). If a cracker has tried all t he words in a dictionary and remains unsuccessful, he or she will try reversing dictionary words, capitalizing letters, et c. (Schneier, 2000). Finally a cracker will try all character combinations (Schneier, 2000)

1.3 Password Standards

The following sections describe the characteristics of strong and weak passwords according to the Sans Institute Pass word Policy (Sans.org, 2013). Characteristics of Weak Passwords (Sans.org, 2013) 1. The password has less than fifte en characters. 2. The password is a word that can be found in a dictionary (English or foreign). 3. The password is an ordinary word such as a. Names of family, pets, friends, co-
workers, fantasy characters, etc. b. Computer terms or names, commands, sites, companies, hardware, software. c. The words "", "sanjose", "sanfran" or any similar derivation. d. Birthdays and other personal information such as addresse s and phone numbers. e. Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc. f. Any of the above spelled backwards. g. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

1.4 A Strong Passwords has the Following Characteristics (Sans.org, 2013):

1. Contains both upper and lower case characters (e.g., a-z, A-
Z) 2. Contains numbers and symbols as well as letters, for example, 0-
9,!@#$%^&*()_+|~ =\‘{}[]:";’<>?,./) 3. Contains at least fifteen alphanumeric characters. 4. Is not a word in any lang uage, slang, dialect, jargon, etc. 5. Is not based on personal, meaningful information such as names of family, telephon e number, SSN, etc. 6. Is never be written down or stored on-
line. In sum, a good password should be complex but nevertheless easy to remember (Burnett, 2002). A good passwor d should also be long and consist of letters, numbers, and symbols. It should let the user type quickly with few errors (Burnett, 2002). Most importantly, a good password should appear random yet be familiar and meaningful to the user (Burnett, 2002). The best password policy is the one that enables the user to create these passwords (Burnett, 2002). H owever, the recommendations of most password policies are not always practiced by users or enforced (B.DawnMedli n & Cazier, 2005).

1.5 How Secure Are Passwords?

The measure of disorder is called entropy (Schneier, 2000). In other words, the more entropied something is, the more uncertainty there is in that particular thing (Schneier, 2000). For instance, if we choose a random person from any po pulation, we will choose either male or female (Schneier, 2000). That indicates that the gender variable has one bit of entropy (Schneier, 2000). Most people who create cryptographic algorithms consider 128 bits to be strong (Schneier, 2 000); however, this is not the same thing as entropy (Schneier, 2000). This is because 128 bits is not a measure of ran domness, but the key length that measures the maximum amount of work that a hacker or cracker must do to break the algorithm and obtain the key (Schneier, 2000). One hundred and twenty-
eight bits indicates nothing about the minimum (Schneier, 2000). Most keys are generated from passphrases or passwo

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

rds (Schneier, 2000). An information system that accepts 10-character ASCII passwords has 80 bits to represent; however, it has less than 80 bits of entropy (Schneier, 2000). Standard English has approximately 1.3 bits of entropy per character (Schneier, 2000). A password with 8 characters has the same entropy as a 32-bit key length (Schneier, 2000). Thus, to arrive at a 128-bit key length, an English-speaking individual would be required to use a 98-character passphrase (Schneier, 2000). Notably, Windows' algorithms, which its designers consider to be quite strong, accept a 128-bit key length (Schneier, 2000). However, the entropy in the password is far lower than that (Schneier, 2000). Password-cracking software will not try every possible key in order (Schneier, 2000). It will try the most likely password first and then try the rest based on probability (Schneier, 2000). For instance, a brute force password-cracking software in figure 1 will try common passwords such as "password," "admin," or "1234" first; then it will try the entire English dictionary; and then varied capitalization, numbers, and other symbols (Schneier, 2000). The program described in the previous section is called L0phtcrack.

A dictionary-attack method such as L0phtcrack used to be difficult because computers were slow (Schneier, 2000) but is a lot easier now because computers today are much faster than those in the past (Schneier, 2000). For passwords with 7 characters in WindowNT, "L0phtcrack can try every alphanumeric password in 5.5 hours, every alphanumeric password with some common symbols in 45 hours, and every possible keyboard password in 480 hours" (Schneier, 2000, p. 137). Moreover, Moore's Law has made it easy for a cracker to use the brute force method on long entropy keys (Schneier, 2000). Simultaneously, there is a maximum to the entropy of passwords that end users can or are willing to remember (Schneier, 2000). Considering that end users would have to memorize a 32-character random hexadecimal string to have a password equivalent to a 128-bit key (Schneier, 2000), it is not difficult to see why most people either opt for weaker passwords that are more easily memorizable or write them down.

II. LITRATURE REVIEW

2.1 Password Attributes

Zviran and Haga (1999) conducted a survey on computer users at a Department of Defense installation in California. Questionnaires were returned by 997 participants. Zviran and Haga (1999) observed that 24.9% of the respondents had 6 characters in their passwords. Zviran and Haga (1999) also observed that 80.1% of the respondents' passwords consisted of only alphabetic characters. Zviran and Haga (1999) observed that most user-selected passwords are derived from the characteristics of personal details meaningful to the individual, are fairly short, are made up of alphanumeric characters, are seldom changed, and are frequently written down. In other words, passwords remain easy to memorize and simple in structure and construction. Zviran and Haga (1999, p.179) observed the following: 1. Password selection methods affect password memorizability. 2. The increased frequency of changing a password, even though it increases the level of security, hinders memorizability. 3. The more frequently a password is used, the less often it is written down. 4. The more a password is used, the less difficult it is to remember. 5. Changing passwords frequently, although necessary to reduce password predictability, hinders recall. 6. Difficulty recalling a password is related to a user's tendency to write it down. 7. Difficulty recalling a password or writing it down is not related to a password's length. 8. Whether a password was chosen to make it easy to remember has no bearing on whether it is written down. Zviran and Haga (1999) urge replication of their findings in future research to challenge these findings in various user populations and organizations to enhance their generalizability.

2.2 End User Security

When users are allowed to select their own passwords, they tend to select passwords that are easy to remember but also easy to crack (Adams & Sasse, 1999). End users prefer passwords that are short, simple, and derived from meaningful details (Adams & Sasse, 1999). Like Zviran and Haga (1999), Adams and Sasse (1999) observed that some users create their passwords based on details meaningful to them. This potentially includes variations of their own or a relative's name, a pet's name, street address, birth date, social security number, etc. (Adams & Sasse, 1999). They also observed that user knowledge regarding secure password content is not sufficient (Adams & Sasse, 1999). Most end users d

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

o not know how to create a secure password, and they do not know how serious it can be if their passwords are compr omised (Adams & Sasse, 1999). Adams and Sasse (1999) posit that, without instruction from IT experts, end users oft en create their own rules for inventing passwords, which are thus often not secure. Passwords that can be derived from the dictionary (real words) are extremely easy to crack from a hacker's perspective (Adams & Sasse, 1999). Most use rs do not know how password cracking works (Adams & Sasse, 1999).

2.3 Using Passwords Multiple Times

Although password theft is a danger to the information system in which a password is compromised, password theft c an also threaten other information systems (Ives, Walsh, & Schneider, 2004). Because many people have multiple pass word-
protected accounts and they often reuse identical passwords repeatedly, hackers can more easily gain access to other a ccounts (Ives et al., 2004) For example, if a hacker gains access to a poorly protected departmental file server and the passwords are compromised, those passwords can be used to gain access to a more securely protected corporate syste m (Ives et al., 2004). This is referred to as a "domino effect" (Ives et al., 2004). A domino effect is the result of one si te's password file being compromised by a hacker who then uses it to penetrate other information systems (Ives et al., 2004).

2.4 Organizational Problems

There is a major gap between end users and IT experts (Adams & Sasse, 1999). End users do not understand security i ssues whereas IT security departments do not understand end users' perceptions, tasks, and needs (Adams & Sasse, 19 99). That is why IT departments view end users as security risks who need to be managed and controlled. Users may b e perceived as the enemy within (Adams & Sasse, 1999). Conversely, users view security mechanisms as laborious ov erhead that can get in the way of their work (Adams & Sasse, 1999). Adams and Sasse (1999) also observed that an or ganization sometimes advocates the sharing of passwords to maximize convenience in the work process.

2.5 Social Problems Sasse et al (2001)

observed that sharing passwords is considered a sign of trust among colleagues and friends. People who are not willin g to share passwords with colleagues are regarded as "untrusting" (Sasse et al., 2001). Users who practice safe comput ing by having strong passwords are often described as "paranoid" or "antisocial" (Sasse et al., 2001).

2.6 Memorizability

Miller (1956) indicates that human short-term memory can store only seven plus or minus two (7+/-
2) chunks or amounts of information. However, this rule applies to information that must be recalled without rehearsa l (Hewett, 1999). Information can be memorized for a long period if it is rehearsed (Hewett, 1999; Newell & Simon, 1 972). In addition, Sasse, et al. (2001) note the following: • The human memory is limited. • Human memory can decay over time. • Frequently used passwords are easier to memorize than less frequently used passwords. • Humans cannot "forget on demand," which indicates that some items (passwords) are still in the memory even though they are not ne eded. • Passwords that are meaningful are easier to remember than non-
meaningful passwords. • Different items can be related to one another to assist recall. Nonetheless, related or similar it ems can compete with one another for recollection. Adams and Sasse (1999) observed that users' having many passw ords can affect the passwords' memorizability. When users are assigned a cryptographically strong password such as " Da*3?^43jC", they will forget it; thus, they tend to write it down (Warkentin, Davis, & Bekkering, 2004). In addition, currently, end users must remember too many passwords. The evolution of ecommerce has resulted in a massive incre ase in the number of passwords required by end users (Ives et al., 2004). When the user cannot remember every passw ord, he or she will generally write them all down, which, of course, is considered an insecure practice because the pass words can be stolen or lost more easily.

2.7 Three Stages of Memory

According to Higbee (2001), there are three stages of memory: 1. Acquisition or encoding is learning or studying the material in the first place, or as Anderson defines it, "how a permanent representation of the information is encoded an d how this record is strengthened" (Anderson, 1994, p. p.191). In the case of passwords, the acquisition process occurs

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

when the users construct the passwords or they are assigned to the users in the first place. 2. Storage is keeping the m aterial until it is needed. Storage, or retention, is "how the information is maintained in memory" (Anderson, 1994, p. p.191). In the case of passwords, the storage process occurs when the users memorize the passwords. 3. Retrieval is id entifying the material and getting it back out when it is needed. Retrieval is "how the information is brought out of me mory when needed" (Anderson, 1994, p. p.191). In the case of passwords, the retrieval process occurs when the user r ecalls the passwords.

2.8 Short-Term Memory

In general, most people cannot remember more than 7 digits (Higbee, 2001). A few people can remember 10 or 11 dig its (Higbee, 2001), and a very few people can remember more than 11 digits (Higbee, 2001). Short-
term memory refers to "how many items can be perceived at one time or how much a person can consciously pay atte ntion to at once" (Higbee, 2001, p. 19). If the person does not have a systematic manner in which to memorize inform ation, information storedin short-
term memory is forgotten in less than 30 seconds (Higbee, 2001). That suggests that when a person acquires his or her password, the decay process is already occurring. However, the typical method of preventing this is rehearsal, which can serve two purposes: 1) it can retain the information in short-
term memory or 2) it can help people transfer the information into longterm memory by giving them time to code it (Higbee, 2001). The rehearsal in the case of passwords is the frequency of use and is a component of the training menti oned in Chapter 4.

2.9 Long Term Memory

According to Higbee (2001), there are three types of long-
term memory: 1. Procedural memory, or how one memorizes how to do something (skills such as typing); 2. Semantic memory, or how one memorizes factual information (such as math equations or word meanings) or in our case, passw ord memorization; 3. Episodic memory, or how one memorizes personal events (such as a person's first date or where someone learned a particular equation). The following diagram describes how memory works and the relation between short-term and long-term memory based on Atkinson and Shiffrin's theory:

The challenge of this study is how to transfer a password from short-term memory to long-
term memory. There are several techniques and strategies that can aid in this transfer. The techniques and strategies ar e mentioned in chapter 4.

2.10 Five Reasons People Forget (Higbee, 2001)

1. Decay. Materials are not used. In the case of passwords, forgetting the passwords is caused by not using them or us ing them infrequently. 2. Repression. Unpleasant or unacceptable memories can be deliberately forgotten. In the case of passwords, the users may simply refuse to memorize a password because they do not like the password policy or do not like the assigned password. 3. Distortion. People remember some things the way they want to remember them. In the case of passwords, people may create their own systems of remembering the passwords, and those new systems m ay distort their memorization. 4. Interference. Information people have learned in the past may interfere with their me mory of something they have learned recently (proactive inhibition). In the case of passwords, old passwords may inte rfere with the memorization of a new password. Information people have learned recently may interfere with their me mory of something they learned in the past (retroactive inhibition). In the case of passwords, the new passwords may i nterfere with the remembering of old passwords. 5. Cue dependency. Memory relies on identifying the right cue to ret rieve what was memorized. In the case of passwords, recalling the passwords depends on identifying the right cues, su ch as questions and answers, to be able to recall them.

2.11 How Fast Do People Forget?

Research on memory indicates that a person does not forget at a steady rate, that most memory loss occurs after learni ng; the rate of forgetting slows down and levels off as time passes (Higbee, 2001). Hence, the largest amount of what people forget will occur shortly after they have learned the information (Higbee, 2001). That suggests that the highest rate of forgetfulness occurs right after people acquire their passwords. However, the exception to the rule is that mater ial that is learned systematically or that is extremely important may be retained in the memory for a long time (Higbee

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

, 2001). Consequently, if the person learns how to remember the password systematically and if the person perceives p asswords as important, he or she will be able to remember them for a long time.

2.12 The Basic Foundation of Memorization (Higbee, 2001)

1. Meaningfulness. The more meaningful the material is, the easier it will be to learn and remember. In his experiment , Anderson (1994) observed that "subjects tend to remember the meaning of a text rather than its exact wording" (And erson, 1994). For instance, words grouped into meaningful categories are easier to remember than words presented in meaningless order. 2. Familiarity. The more people know about a particular subject, the easier it is to learn new infor mation about it. In the case of passwords, the old password is easier to recall than the new password. 3 Rhymes. Many people use a rhyme to help them remember information. An example of a rhyme is the Alphabet Song ("AB-CD-EFG . . ."). 4. Patterns. If people can discern a pattern, rule, or underlying principle in the material, they will likely be able to learn it more easily. To render information more meaningful, patterns serve to chunk the material so there is le ss to remember. If people can see a pattern, then all they must memorize is the pattern, which will allow them to gener ate the original material. 5. Organization. If the material is organized, it will be easier to memorize. The position of th e material also plays a role in memorization. Research indicates that the order in which items are organized can affect how easy they are to learn and memorize.

6. Association. Association involves relating what people want to learn to something they already know. This method can be accomplished by analogy. For instance, people can associate their passwords with what they are already familia r with such as familiar numbers, dates, or specific events.

7. Repetition.

Repetition is the frequency of using the passwords. Users can use the repetition method to improve the memorizabilit y of passwords by frequently using their passwords or by rehearsal.

III. RESEARCH METHOD

The survey was used to analyze the current characteristics of users' behavior in utilizing their passwords.

IV. FINDINGS

The survey was sent to executive MBA students at one of the AACSB accredited business schools in Thailand. Of 90 students, 63 responded to the survey. Of the respondents, 46 (73%) were female, 17 (27%) were male, and 63% (40 s tudents) were between 26 and 30 years old. Nineteen per cent (12 students) were between 31-
35 years old, and 37 students (37%) worked for a private company. Sixteen per cent were entrepreneurs, and 14% wor ked for the government. Ninety-
five per cent mentioned that they had an account with the information systems in their workplace. When asked about t he number of characters in their passwords, the majority (29%) had 8 characters, 10% had 9 characters, 15% had 10 c haracters, 12% had 11 characters, and 7% had fewer than seven characters in their passwords. Of the respondents, 11 % had only numbers in their passwords, 30% had both characters and numbers in their passwords, and 17% had chara cters, numbers, and symbols in their passwords. When asked how they had created their passwords, 33% of the respon dents responded that they thought of some name or date that has personal significance for them such as the name or bi rth date of a family member. Some (28%) combined entire or partial names, dates, words, and numbers to create a stri ng of characters that they could remember such as "Jane2005" or "mycode7". Eleven per cent mentioned they would t hink of a word that is easy to remember, such as "basketball" or "accounting". Only 10% mentioned that they would make up "nonsense" strings of letters, numbers, and symbols such as "T3%x&W9" or "GhW4q$p". When asked how often they used their passwords to log in to the company's systems, more than half (65%) said that they logged in to t he company's systems many times a day; 18% only logged in once a day. When asked how many systems they used (other than their company's system) that required a password, 40% reported using 4 systems, and 15% reported using f ive systems. When asked how many distinct passwords they used for all systems, only one person reported using only one password for all systems, 29% used two passwords for all systems, and the majority (41%) used three passwords f or all systems. When asked if they had ever used their company's passwords for any other systems, 50% (30 users) ad mitted they used company's passwords for other systems such as email, social networking, and other website registrati on. When asked if they ever wrote down their passwords or stored their passwords in their computers, 37% (15 users)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

admitted writing down or storing their passwords in the computer. In addition, when asked if anyone else used their w ritten passwords, 28% (17 users) admitted allowing other people to use their written passwords. Nearly half (43%) ad mitted that they have shared their company's passwords with friends or colleagues; 42% of the users reported changin g their company's passwords because they suspected that the passwords had been compromised or guessed by someon e else.

When asked how often they changed their passwords, more than half (51%) reported never changing their passwords, and 23% reported changing their passwords every three months.

V. DISCUSSION

Passwords are still one of the weakest links in information systems because people use weak passwords. According to the survey, nearly eighty percent of users have fewer than ten characters in their passwords, and more than half of the respondents reported having only characters in their passwords. With the current password-
cracking software, these passwords are easy to crack in a matter of seconds. The results of this study also show that pe ople often create passwords based on their personal information such as birthdates, citizen id, telephone number, and f amily members' names. These passwords can be easily guessed by friends and colleagues. Another problem that I obs erved in the results of this study is people often reuse passwords. Nearly everyone in the study reported that they have only between two and three passwords to access every account. This can lead to the domino effect problem in which t he hacker can gain access using one password and then use the same passwords for other accounts. Sometimes, the ha ckers do not even need to hack the password. They can set up a website and ask users to register with a username and password. Some people will reuse the same password that they use with other accounts such as email, their company's systems, and e-
banking accounts. Once the hacker has a user's password, he or she can use the same password with other systems inc luding users' email and e-
Banking account. In this study, the results present the contrast between strong passwords and memorization. Miller (1 956) posits that human short-
term memory can store only seven plus or minus two chunks of information (Miller, 1956), and unless a person devel ops a systematic way to memorize that information, it will be forgotten in less than 30 seconds (Higbee, 2001). This fi nding is consistent with the research documents used in creating the study, indicating that the longer a password is, the more difficult it is to remember (Sasse et al., 2001; Schneier, 2000; Warkentin et al., 2004; Zviran & Haga, 1999). W hen the users cannot memorize the passwords, the solution is for them to write the passwords down. In this study, near ly half of the respondents indicated that they wrote down their passwords to aid their password memorizability. Sharin g passwords is common practice in IS organizations (Sasse et al., 2001). Passwords are supposed to be secret; thus, sh aring them defeats the purpose of having them, making it next to impossible to verify who the users are in the system or to account for what went wrong with the system (Sasse et al., 2001). The main reason users share their passwords i s for convenience. In this study, the results indicate that nearly half (43%) admitted that they have shared company pa sswords with friends or colleagues. Finally, the results indicate that most users never change their passwords. This can create a serious problem because most users do not know if their passwords have already been compromised. The hac ker can use compromised passwords to access users' accounts without the users' knowledge.

VI. CONCLUSION

Passwords are the first line of defense in any information system; however, their importance has been ignored by both practitioners and researchers. The literature related to password security indicates that a strong password that is long, complicated, and not derived from personal, meaningful details is difficult to remember and weak passwords that are s hort, simple, and derived from personal, meaningful details are easy to remember (Schneier, 2000; Warkentin et al., 2 004; Zviran & Haga, 1999). When users cannot memorize a password, the solution is to write it down (Sasse et al., 20 01; Schneier, 2000; Zviran & Haga, 1999). A written password can be lost or stolen. In addition, when users cannot m emorize numerous passwords, they often reuse the same password multiple times. If hackers can gain access to one ac count, they may be able to gain access to other accounts (Ives et al., 2004). Memory literature indicates that humans h ave a limited capacity for memorizing information (Higbee, 2001; Miller, 1956). Information stored in long-
term memory can be memorized for a longer period than information stored in short-
term memory (Higbee, 2001). The findings of this study support previous findings in the literature that end users use

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010096|

weak passwords. The majority of users write down their passwords. Most users reuse a password for multiple account s. Most users share their passwords and never change them. IT security must develop both technical and policy solutio ns to address the problems of users' behavior in utilizing passwords; otherwise, passwords will continue to be a weak link in information systems.

REFERENCES

[1] Anderson, J. R. (1994). Learning and Memory: An Integrated Approach: John Wiley & Sons Inc [2] B.DawnMedl in, & Cazier, J. A. (2005). An Investigatieve Study: Consumers Password Choices on Journal of Information Privacy & Security, 1(4), 44.

[3] Burnett, M. (2002, March 7, 2002). Ten Windows Password Myths Retrieved April 12, 2005, from http://www.se curityfocus.com/infocus/1554

[4] Ives, B., Walsh, K. R., & Schneider, H. (2004). The Domino Effect of Password Reuse. Association for Computin g Machinery. Communications of the ACM, 47(4).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details