# The One-Eyed Leading the Blind: Understanding Differences Between IT Professionals and Non-IT Staff When Creating and Managing Passwords

Paul Brockbanks, Martin J. Butler

# The one-eyed leading the blind: Understanding differences between IT professionals and non-IT staff when creating and managing passwords

Paul Brockbanks[1] and Martin J Butler[1] [0000-0002-5232-781X]

[1] Stellenbosch University, Stellenbosch, South Africa
martin.butler@usb.ac.za

**Abstract.** Passwords remains the standard mechanism by which organisations protect their data from unauthorised entities accessing, changing or misusing their information. Organisations go to great lengths to educate their workers on the importance of creating and maintaining secure passwords.

Extensive research has been conducted on how users create and manage their passwords. To date, there is limited insight on how the behaviour of IT workers may differ from that of non-IT workers. It is generally assumed that IT workers have a greater understanding of what a secure password entails and how insecure password behaviour may put an organisation's resources at risk by the nature of their roles. Consequently, they are expected to have a positive influence on non-IT workers' password behaviour.

This research sets out to test this assumption. The findings suggest significant differences between the password practices applied when IT and non-IT workers create and manage their passwords. However, poor security behaviour by both IT and non-IT workers was evident.

**Keywords:** human behaviour, IT, non-IT, passwords, security, password-fatigue, users.

## 1 Introduction

Passwords remain the most common control mechanism for authenticating a user's identity when accessing a system [1]. It serves as the first line of defence against unauthorised access [2]. Passwords are generally governed by specific criteria that should be used to secure passwords and improve security [3].

Employees working outside the IT function often turn to their colleagues in the IT department to create strong passwords and help manage them [4]. The different roles of non-IT and IT workers may contribute to differences in their understanding of security issues [5]. It was suggested that IT workers better understand access rules' value and purpose than other users [6]. By the nature of their role, IT workers may have had more exposure to password security best practices than non-IT workers. IT workers implement and monitor the security policies and have extensive system access, and should have increased awareness of what constitutes a safe password and how to secure it properly [7].

However, IT workers may not be as security-conscious as expected. Despite their assumed additional password security awareness, it may be possible that IT workers are a 'weak link in the chain'. This study aimed to investigate whether IT workers applied more secure password practices than non-IT workers.

## 2 Prior research

### 2.1 User generated passwords

The growing dependence on systems that contains sensitive data has given rise to individuals or groups that seek to access this information with malicious intent [8]. Although user passwords have been the cornerstone of authentication for over 50 years, very little has changed regarding the user experience [9]. A user typically logs onto a system by providing a unique identifier and password. The security mechanism then verifies the match between the user identifier and the password; if both are correct and valid, the user is granted access to the system [10].

The strength of a password lies in its resistance to malicious activities [11]. A password is only useful to the extent that it denies access to organisation assets to adversaries [12]. For example, the greater the length and the larger number of different characters, the more resistant the password will be [3].

The composition of passwords also contributes to their strength. Passwords based on dictionary membership or containing repeated characters or consecutive sequences, are weaker and may be easily guessed [13]. There are nearly three trillion possible eight-character password combinations using the 26 letters of the alphabet and the numerals 0 to 9 [14]. Despite this large pool of possibilities, users prefer to create easy to remember passwords [15].

Kaplan-Leiserson [16] suggested that 70% of security breaches were indirectly or directly due to staff's actions within companies. The 2020 Data Breach Investigations report [17] clarifies that although most threat actors are external to the organisation, they often exploit internal staff vulnerabilities.

These vulnerabilities could include poor password creation practices (e.g. creating passwords that are easy to guess), poor password management practices (e.g. reusing passwords), or falling victims to social phishing. Although the threat actors may be external, they exploit employees insecure practices, damaging consequences for organisations [18].

### 2.2 Defining and categorizing password practices

Butler and Butler [19] separated password activities into creation and management practices (Figure 1). Although this presents a valuable lens to analyse the different practices, not all user actions fall distinctly into either creation or management activities. For example, the practice of reusing passwords does not fit uniquely into these categories since it is a password management practice, but the application manifests during passwords creation. As such, password reuse measures are defined as creation and management activities (refer to Figure 1 and Table 1).

Password policy restrictions may include users having to choose passwords that contain characters outside of the 26-letter alphabet, uppercase characters, lowercase characters, digits and symbols. When users create passwords, dictionary membership may also be automatically checked by the system to ensure that no common passwords are created [20]. Policy restrictions often enforce more secure creation practices. Password management rules guide users to manage their passwords securely, once created. It is more difficult, if not impossible, to measure the level of compliance with management practices [12].

Florêncio et al. [11] observed that usability imperatives played a role in implementing an organisation's password policies. Kelley et al. [21] questioned the use of strict policies by suggesting that administrators have steadily increased the requirement for more complex passwords, even when the value thereof is poorly understood. Password policies may have been created decades ago when it was assumed that minimum length and complex character sets made it more difficult for passwords to be guessed [22].

Hicock [23] challenged some conventional beliefs and indicated that several policies might be unnecessary or too onerous for the user. The term 'anti-patterns' was adopted to describe these common but questionable security practices [24]. Examples of anti-patterns include the belief that passwords should contain multiple character sets, including the need for passwords to consist of a combination of uppercase, lowercase and numeric characters. It is suggested that this approach is not practical as threat actors looking to guess passwords have already included substitutions in the standard dictionary. Toulouse [25] supports Hicock's view by highlighting, in his view, the much-needed shift from a purist approach that relies exclusively on complex and strict rules to an approach that recognises the challenges that users face when trying to manage passwords more efficiently while keeping them safe.

The challenge of conventional views on security practices extends to the management practices as well. For example, Herley [26] argues that preventing users from writing down passwords increases the user's burden, whilst offering marginal security gain in return. Zhang-Kennedy [12] support this view by suggesting a significant usability gain by allowing a practice that presents a slight security risk. Examples of this gain include the increased ability of users to create multiple passwords across different systems and provide a mechanism to allow users to compose more complicated passwords [27].

Despite these valid questions about common passwords security believes, in this article, and aligned with the data available for analysis, the conventional beliefs about stronger passwords and more desirable management practices are used to analyse the difference between the practices applied by IT and non-IT users.

### 2.3 Unsafe passwords creation and management practices

Users continue to adopt methods that may not be secure, despite being provided with security guidelines and policies [28]. Undesirable password creation practices include more complex and longer passwords and not using common words or numbers that can be easily recognized [29]. The management practices that are not desirable includes writing down and sharing passwords.

According to Adams, Sasse and Lunt [30], writing down passwords started when it became customary for users to receive a system-generated password that was difficult to remember. Adams and Sasse [31] suggested that whilst system-generated passwords provided the optimal security approach, user-generated passwords were potentially more memorable and less likely to be written down. The writing down of passwords has conventionally been seen as an insecure practice [32]. It is one of the many risky behaviours that undermine system security [33]. Nearly four decades ago, Porter [34] Porter (1982 suggested that once one has written down a password, it is no longer a password.

However, recording passwords as a security practice is not as generalizable as it would seem at first glance. Although users may think that password rules are complex and write down passwords to remember them, there are secure ways to achieve this without compromising security [35]. For example, using a password manager or keeping a written down password in safekeeping could be desirable if correctly applied by users [36].

As with the reuse and writing down of passwords, sharing passwords has conventionally been seen as a risk to system security [31]. Sharing of passwords defeats the underlying purpose of the identification process [12]. Adams and Sasse [31] dams and Sasse (1999) noted that passwords were often shared among work colleagues and friends due to practical and convenience reasons. Weirich and Sasse [33] suggested multiple reasons why users may feel compelled to share passwords, such as circumstances at work necessitating sharing a password to enable a colleague to access the system on their behalf or being pressured to share their passwords by a superior. Users may also feel safe providing passwords to those more technically capable than themselves when seeking support with a task or needing technical assistance. The inability to memorize the increasing number of passwords is no doubt a contributing factor to sharing passwords [37].

Although the reuse of passwords is common among users, it may allow a threat actor to access many systems with one password [32]. A password initially created on a low-security system may ultimately be used on a secure system that contains confidential information [38]. Ives and Walsh [39] refer to this as the 'Domino Effect', highlighting that once the weakest password has failed, other systems accessed may provide more password information that, in turn, may cause more systems to be compromised.

## 3 Research problem and objectives

Business managers find the impact of security policies on productivity more important than IT professionals, whose primary concern appears to be the system's security [40]. However, Shay et al. [41] suggest that IT users are less likely to share their passwords than non-IT users and prefer security policies that are more stringent than more user-friendly policies that may have fewer security attributes.

Both IT and non-IT users expressed overall dissatisfaction with the state of current password rules but differed on the reasons for this dissatisfaction. IT users were more likely to indicate that IT policies were thought through and sensible [42]. However, both sets of users suggested that they could envisage scenarios where they would circumvent security rules.

Loutfi and Jøsang [7] suggest that IT professionals' tacit knowledge of safe passwords practices does not always translate into safe practices. IT professionals used unsafe methods to store passwords and did not create complex passwords unless forced to do so [7]. One area that IT users appeared to perform well in was memorising longer passwords (more than eight characters). The authors concluded by suggesting that whilst IT users were aware of what constituted correct password behaviour, in many instances, they failed to translate this awareness into practice.

Although numerous studies have been conducted to understand users' behaviour and their motivation when creating or safeguarding their passwords [43], it is unclear whether IT workers, who may be seen as setting the standard, really possess greater knowledge or behave more securely than non-IT workers. This study's primary objective was to compare how IT and non-IT workers create and manage their user-generated passwords.

## 4 Research methods

The focus on security awareness within financial services institutions made it an ideal environment for research focusing on how IT and non-IT workers secured their user-generated passwords. IT workers were defined as those with a direct technical executions responsibility, that forms part of the organisation's IT department. The grouping of IT users includes all the different IT roles and is not limited to security professionals. Respondents not within the IT services organisations were classified as non-IT users.

The financial institution selected for this research conducts regular IT security awareness campaigns and surveys. The data collected through surveys is used to ascertain IT security awareness amongst the staff and determine the need for awareness campaigns. The organisation surveyed employees to understand how they secured their user-generated passwords. Confidentiality is ensured by restricting responses to predefined options and not collecting any information that may be linked back to an employee. Data collected as part of the original survey was made available to the researchers after obtaining ethical clearance.

An inferential analysis follows a descriptive study to test for a significant difference between IT and non-IT workers in securing their passwords. The data contained responses from 182 employees, of which 118 (65%) were classified as non-IT users and 64 (35%) as IT users. The data were analysed through t-tests that checked for significant difference (p-value < 0.05) between IT and non-IT users' responses.

# 5 Research results

## 5.1 Descriptive analysis

Figure 1 depicts the descriptive data indicating poor password practices among IT and non-IT users. The data (that is more granular than presented) contained responses both in the negative (non-desirable action or lack of action), and the positive (desirable action or absence of non-desirable action). The detailed data was summarised to provide a single measure in the negative (higher result is less desirable) for descriptive purposes. Only 19% of the IT user group reported *using random characters* in their passwords. Within the non-IT user group, 11% of the users reported using random characters in their passwords. Both IT (49%) and non-IT (52%) users *included descriptive names* when creating their passwords.

Within the IT user group, 39% of the users reported *using sequential numbers or dates* in passwords. Whilst there is a significant difference with 57% of non-IT users engaging in this insecure practice, any use of sequential numbers is a security risk. Patterns in passwords created using recognisable number combinations may enable language-independent password guessing algorithms to exploit passwords that can be used to gain successful entry into systems (Veras, Collins, Veras, Thorpe & Collins, 2012).

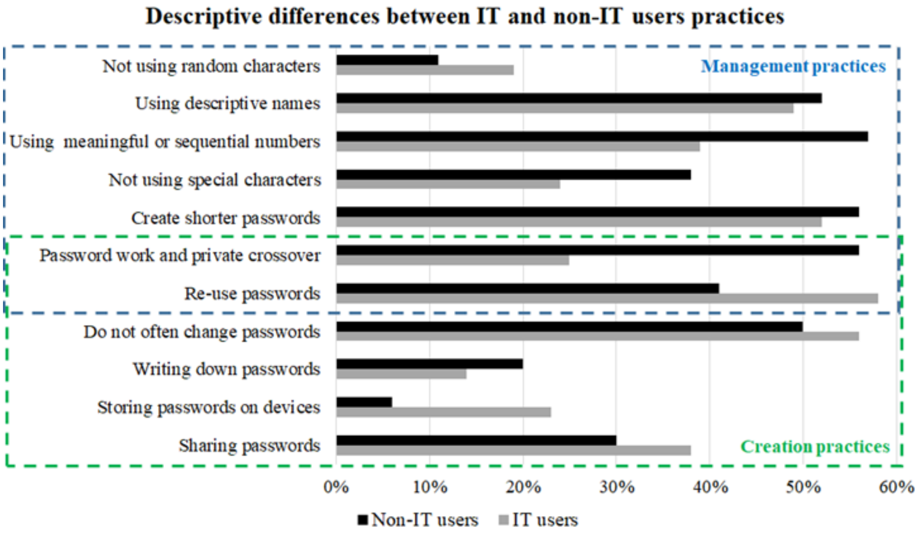

**Fig. 1.** Descriptive difference between IT and non-IT users (n = 182)

A total of 76% of IT users reported *using special characters* (i.e. %$_*#) compared to 62% of the non-IT user group. In terms of *password length*, IT-users outperformed non-IT-users significantly with 44% versus 20%, respectively creating passwords of nine characters or longer. It is plausible that IT-users may have developed methods like passwords phrases to remember long passwords.

One significant difference is using passwords for *both private purposes and access to work systems*. Within the IT user group, 25% of the users used the same or a similar password in the workplace as they did in their private capacity, compared to 56% in the non-IT user group. Similarly, both IT (69%) and non-IT (62%) users *reused passwords* across some or all of their applications. Once one particular password has been breached, other applications that use the same password become vulnerable.

Both IT (58%) and non-IT (41%) users indicated that they reused the same or similar passwords when creating new passwords. Password reuse may be caused by the number of different passwords that users must create and the challenge to remember them [31]. Password expiration policies may also contribute to password reuse. Hicock (2016) challenged the use of password expiration policies since they may force users to create more predictable passwords that include sequential words.

IT-users *change their passwords* more frequently than non-IT users and are less likely to write them down. Within the IT user group, 14% of the users reported *writing down their passwords*, and 20% of the non-IT user groups did. Both IT (23%) and non-IT (6%) users indicated that they *stored their passwords* on devices. Storing passwords on other devices is a common practice amongst users and may be a safe way of keeping track of passwords, as long as these devices cannot be accessed by another user [12]. Given that no further data about these devices being available, this study defines it as an unsafe practice.

Both IT (38%) and non-IT (30%) users indicated that they *shared their passwords* with other users. Zhang-Kennedy et al. [12] suggest that the sharing of passwords defeats the underlying purpose of the identification process, maintaining a one-to-one mapping of the users' identification and the data that they are authorised to access.

### 5.2 Inferential analysis

The primary objective of this study was to compare how IT and non-IT workers secured their passwords. It is evident from Table 1 that there is no significant difference between IT and non-IT users' behaviour in five of the eleven data points measured, whilst six indicate a significant difference between IT and non-IT users.

A trend is evident once the practices are categorized as creation and management practices. In all instances of significant differences in creation practices, IT users displayed more desirable practices and could provide more secure examples and guidance. However, when investigating the two management practices where a statistical difference exists, non-IT users display the more desirable behaviour.

IT-users thus do not practice examples to follow, or may not be able to provide correct guidance, unless other factors lead to their less secure behaviour, for example, the burden to have more passwords. However, it is concerning that IT users' passwords with system-level access may conceivably provide access to more valuable information resources.

**Table 1.** Inferential differences between IT and non-IT users (n = 182).

| Practice group | Criteria tested | Statistically significant | P value | More desirable behavior group |
|---|---|---|---|---|
| Creation | Password length | Yes | 0.00003 | IT users |
| Creation | Using descriptive names | No | 0.75618 | - |
| Creation | Using meaningful or sequential numbers | Yes | 0.01938 | IT users |
| Creation | Not using special characters | Yes | 0.04412 | IT users |
| Creation | Using random characters | No | 0.13797 | - |
| Creation & Management | Password work and personal cross-over | Yes | 0.00002 | IT users |
| Creation & Management | Reuse passwords | Yes | 0.02810 | Non-IT users |
| Management | Not regularity changing passwords | No | 0.30239 | - |
| Management | Writing down passwords | No | 0.31091 | - |
| Management | Storing passwords on devices | Yes | 0.00232 | Non-IT users |
| Management | Sharing passwords | No | 0.25127 | - |

One plausible cause for poor password practices is password fatigue, measured by questions on the number of passwords to be remembered. Within the IT user group, 18% needed to remember more than ten passwords, compared to only 2% in the non-IT group. When analysing the detailed data, there was a statistically significant difference ($p > 0.001$) in the number of workplace passwords used between IT and non-IT users, indicating that IT users may be under more pressure to use less secure coping mechanisms.

## 6 Managerial implications and recommendations

Prior research suggests that IT workers' assumed knowledge of safe password practices does not always translate into safe practices [7]. This research supports this suggestion and advises that both IT and non-IT workers engage in insecure password creation and management practices.

Organisations need to continue focusing on external security threats exploiting internal weaknesses that expose their assets to potential security breaches. Organisations should acknowledge and correct perceptions that differences in roles between IT and non-IT workers may contribute to differences in their security knowledge and practices. Therefore, we recommend that managers ensure that sufficient and equal attention is paid to IT and non-IT workers whilst educating them on the importance of password security. Organisations should not blindly rely on IT workers to educate non-IT workers on safe password practices.

The research highlights a potential link between the number of passwords that a user must remember and users' coping mechanisms. In the omnipresence of online systems requiring authentication credentials, IT-users' insecure behaviour could be linked to password fatigue. It should serve as a warning for organisations exposing non-IT employees to an increasing number of systems. The findings suggest that using coping mechanisms, such as password reuse and storing passwords on devices, may be avoided if employers limit the number of passwords they require their workers to use.

The general assumption that IT workers apply more secure password behaviours than non-IT workers may be incorrect. This assumption may be placing organisations at financial and reputational risk, warranting further research.

## 7 Limitations and future research

The research is limited by the validity of the measures that define poor password practices. It is acknowledged that specific policies traditionally seen as desirable (e.g. longer passwords or regularly changing passwords) are no longer above approach in the current academic discourse.

Some practices like recording passwords need to be defined and measured at a more granular level to improve the robustness of the research. The recording of passwords once for safe storing or in a secure online password manager should instead be viewed as desirable practice and recorded distinct from recording in a non-secure manner. More attention should be given to the constructs that typically define desirable and not desirable behaviours.

In addition, the research does not take into account practices that may vary due to the nature of the information assets being protected. It is also acknowledged that the study was performed in a single company within financial services in South Africa. Since it is plausible that there may be a difference between industries and cultural differences between countries, it is recommended that future sampling to validate the findings use samples covering multiple industries and, if possible, geographic locations.

The research is also limited by not checking for cross-loadings and relationships between specific practices. Additional insight may be gained from different clusters and associations that could explain more behavioural differences.

Given the findings of this research that suggest that IT workers do not generally display more secure passwords practices than non-IT workers, future research focusing specifically on IT workers' behaviours and coping strategies is required. Further analysis of the data may indicate if IT workers are indeed the 'weak link in the chain' or if the increased number of passwords are the drivers of non-secure behaviour.

## References

[1] J. Kävrestad, M. Lennartsson, M. Birath, and M. Nohlberg, "Constructing secure and memorable passwords," *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 701–717, 2020, doi: 10.1108/ICS-07-2019-0077.

[2] E. F. Gehringer, "Choosing passwords: security and human factors," *IEEE 2002 Int. Symp. Technol. Soc. (ISTAS'02). Soc. Implic. Inf. Commun. Technol. Proc. (Cat. No.02CH37293),* no. February 2002, pp. 369–373, 2002, doi: 10.1109/ISTAS.2002.1013839.

[3] R. Butler and M. Butler, "Some password users are more equal than others: Towards customisation of online security initiatives," *SA J. Inf. Manag.*, vol. 20, no. 1, pp. 1–10, 2018, doi: 10.4102/sajim.v20i1.920.

[4] S. Al Awawdeh and A. Tubaishat, "An information security awareness program to address common security concerns in IT unit," *ITNG 2014 - Proc. 11th Int. Conf. Inf. Technol. New Gener.*, pp. 273–278, 2014, doi: 10.1109/ITNG.2014.67.

[5] K. H. Guo, "Security-related behavior in using information systems in the workplace: A review and synthesis," *Comput. Secur.*, vol. 32, no. 1, pp. 242–251, 2013, doi: 10.1016/j.cose.2012.10.003.

[6] V. Kothari, J. Blythe, S. W. Smith, and R. Koppel, "Measuring the security impacts of password policies using cognitive behavioral agent-based modeling," *ACM Int. Conf. Proceeding Ser.*, vol. 21-22-Apri, 2015, doi: 10.1145/2746194.2746207.

[7] I. Loutfi and A. Jøsang, "Passwords are not always stronger on the other side of the fence," *Proc. Netw. Distrib. Syst. Secur. Conf. USEC Work.*, no. February, pp. 1–10, 2015, doi: 10.14722/usec.2015.23005.

[8] A. Kumar and P. Singh, "Information Technology as Facilitator of Workforce," *Bus. Manag. Dyn.*, vol. 3, no. 12, pp. 15–20, 2014.

[9] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Commun. ACM*, vol. 58, no. 7, pp. 78–87, 2015.

[10] M. Bishop and D. V Klein, "Improving System Security via Proactive Password Checking," *Comput. Secur.*, vol. 14, no. 3, pp. 233–249, 1995, doi: https://doi.org/10.1016/0167-4048(95)00003-Q.

[11] D. Florêncio and C. Herley, "Where do security policies come from?," in *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, 2010, p. 1, doi: 10.1145/1837110.1837124.

[12] L. Zhang-Kennedy, S. Chiasson, and P. Van Oorschot, "Revisiting password rules: Facilitating human management of passwords," in *eCrime Researchers Summit, eCrime*, 2016, vol. 2016-June, pp. 81–90, doi: 10.1109/ECRIME.2016.7487945.

[13] T. Hussain, "Passwords and User Behavior," *J. Comput.*, vol. 13, no. 6, pp. 692–704, 2018, doi: 10.17706/jcp.13.6.692-704.

[14] B. Kevin, *Hacking For Dummies*, 4th ed. 2013.

[15] S. R. Obedur, "Strategies for Password Management Master thesis Shazia Rahman Obedur," UNIVERSITY OF OSLO, 2013.

[16] E. Kaplan-Leiserson, "People and Plans: Training's Role in Homeland Securityo Title," *T+D*, vol. 57, no. 9, pp. 66–74, 2003.

[17] A. J. Nathan and A. Scobell, "2020Data Breach Investigations Report," 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf%0Ahttp://bfy.tw/HJvH.

[18] A. Davidson and S. King, "Data Breaches Continue to Rise : How Financial Institutions Can Prepare & Respond," in *Risk Webinar*, 2016, pp. 2–3.

[19] R. Butler and M. Butler, "The password practices applied by South African

online consumers: Perception versus reality," *SA J. Inf. Manag.*, vol. 17, no. 1, pp. 1–11, 2015, doi: 10.4102/sajim.v17i1.638.

[20] D. Florêncio, C. Herley, and P. Van Oorschot, "An Administrator's Guide to Internet Password Research.," in *28th Large Installation System Administration Conference (LISA14)*, 2014, pp. 35–52.

[21] P. G. Kelley *et al.*, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *Proceedings - IEEE Symposium on Security and Privacy*, 2012, pp. 523–537, doi: 10.1109/SP.2012.38.

[22] S. Komanduri, R. Shay, L. F. Cranor, C. Herley, and S. Schechter, "Telepathwords: Preventing Weak Passwords by Reading Users' Minds," *Proc. 23rd USENIX Secur. Symp.*, pp. 591–606, 2014.

[23] R. Hicock, "Microsoft Password Guidance," 2016.

[24] K. Julisch, "Understanding and overcoming cyber security anti-patterns," *Comput. Networks*, vol. 57, no. 10, pp. 2206–2211, 2013, doi: 10.1016/j.comnet.2012.11.023.

[25] S. Toulouse, "On Changing Password Guidance: A Good First Step From Microsoft," *Leviathan Security Group*, 2017. .

[26] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," 2009.

[27] F. Stajano, S. F. Mjølsnes, G. Jenkinson, and P. Thorsheim, *Technology and Practice of Passwords: 9th International Conference, PASSWORDS 2015, Cambridge, UK, December 7-9, 2015, Proceedings*, vol. 9551. Springer, 2016.

[28] L. Tam, M. Glassman, and M. Vandenwauver, "The psychology of password management: a tradeoff between security and convenience," *Behav. {&} Inf. Technol.*, vol. 29, no. 3, pp. 233–244, 2010, doi: 10.1080/01449290903121386.

[29] R. Veras, C. Collins, R. Veras, J. Thorpe, and C. Collins, "Visualizing semantics in passwords : The role of dates Visualizing Semantics in Passwords : The Role of Dates," *Proc. Ninth Int. Symp. Vis. Cyber Secur.*, no. January, pp. 88–95, 2012, doi: 10.1145/2379690.2379702.

[30] A. Adams, M. A. Sasse, and P. Lunt, "Making Passwords Secure and Usable," *People Comput.*, vol. 34, no. 1, pp. 1–15, 1997, doi: 10.1145/99977.99993.

[31] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999, doi: 10.1145/322796.322806.

[32] E. Stobert and R. Biddle, "The password life cycle: User behaviour in managing passwords," *SOUPS '14 Proc. Tenth Symp. Usable Priv. Secur.*, pp. 243–255, 2014.

[33] D. Weirich and M. A. Sasse, "Pretty good persuasion: a first step towards effective password security in the real world," *Proc. 2001 Work. New Secur. Paradig. - NSPW '01*, no. FEBRUARY 2002, pp. 137–143, 2001, doi: 10.1145/508171.508195.

[34] S. N. Porter, "A password extension for improved human factors," *Comput. Secur.*, vol. 1, no. 1, pp. 54–56, 1982.

[35] R. Khatib and H. Barki, "An activity theory approach to information security non-compliance," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 485–501, 2020, doi:

10.1108/ICS-11-2018-0128.

[36] Z. Joudaki, J. Thorpe, and M. Vargas Martin, "Enhanced Tacit Secrets: System-assigned passwords you can't write down, but don't need to," *Int. J. Inf. Secur.*, vol. 18, no. 2, pp. 239–255, 2019, doi: 10.1007/s10207-018-0408-2.

[37] B. Grawemeyer and H. Johnson, "Using and managing multiple passwords: A week to a view," *Interact. Comput.*, vol. 23, no. 3, pp. 256–267, 2011, doi: 10.1016/j.intcom.2011.03.007.

[38] G. Notoatmodjo and C. Thomborson, "Passwords and perceptions," *Conf. Res. Pract. Inf. Technol. Ser.*, vol. 98, no. Aisc, pp. 71–78, 2009.

[39] B. B. Ives and K. R. Walsh, "The Domino Effect of Password Reuse," vol. 47, no. 4, pp. 75–78, 2004.

[40] R. K. Rainer Jr., T. E. Marshall, K. J. Knapp, and G. H. Montgomery, "Do Information Security Professionals and Business Managers View Information Security Issues Differently?," *Inf. Syst. Secur.*, vol. 16, pp. 100–108, 2007, doi: 10.1080/10658980701260579.

[41] R. Shay, P. G. Kelley, P. G. Leon, M. L. Mazurek, N. Christin, and L. F. Cranor, "Encountering Stronger Password Requirements : User Attitudes and Behaviors Categories and Subject Descriptors," *Hum. Factors*, 2010.

[42] R. Koppell, J. Blythe, V. Kothari, and S. Smith, "Beliefs about Cybersecurity Rules and Passwords: A Comparison of Two Survey Samples of Cybersecurity Professionals Versus Regular Users," *Twelfth Symp. Usable Priv. Secur. (SOUPS 2016),* 2016, [Online]. Available: https://www.usenix.org/conference/soups2016/workshop-program/wsf/presentation/koppel.

[43] V. Kothari, J. Blythe, S. Smith, and R. Koppell, "Measuring the Security Impacts of Password Policies Using Cognitive Behavioral Agent-Based Modeling," in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, 2015, pp. 1–9.