The Password You Hope You Never Use: Use Cases for Duress Authentication

Christina Nissen
chfn@itu.dk
IT University of Copenhagen
Copenhagen, Denmark

Oksana Kulyk
okku@itu.dk
IT University of Copenhagen
Copenhagen, Denmark

Abstract

While passwords are the most widely used method of authentication, concerns about duress attacks have emerged because attackers are motivated to gain access to our sensitive data. To mitigate this, researchers have proposed duress passwords, allowing users to signal to a system that they are under duress silently. We conduct a survey ($N = 281$) to investigate users' perceptions of potential use cases for duress passwords. Our findings show that users perceive critical societal systems and institutions as use cases due to potentially high consequences of a successful duress attack. Further, they consider personal accounts, such as banking, to benefit from implementing duress passwords. Overall, our findings pave the way for future research aimed at developing solutions effective against duress attacks.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**; **Usability in security and privacy**;

Keywords

Duress password, Panic Password, Authentication, User Study, Use Cases, Perceptions

ACM Reference Format:
Christina Nissen and Oksana Kulyk. 2025. The Password You Hope You Never Use: Use Cases for Duress Authentication. In *Companion of the Computer-Supported Cooperative Work and Social Computing (CSCW Companion '25), October 18–22, 2025, Bergen, Norway*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3715070.3749266

1 Introduction

In an increasingly digital world, even sensitive data and essential services are now accessible online. These are often protected by passwords, the most widely used method of authentication [6, 7, 19]. However, attackers are also becoming more motivated to obtain the passwords that provide access to this sensitive data and critical services. One potential strategy to acquire these passwords is through duress, where an attacker could force, threaten, or bribe a victim to log in, undermining the confidentiality [9, 17, 20]. In order for a duress attack to be successful, the attacker needs to be either physically present next to their victim or employ techniques like monitoring the device's screen remotely.

To mitigate the problem of duress attacks, the concept of duress passwords [9, 29] has been proposed, allowing the user to trigger a silent alarm during the login process, indicating that they are being forced to authenticate against their will. Consequently, the system is designed such that even though the attacker knows about this feature, they have no way of detecting the alarm. This concept has been used, for example, in the context of electronic voting, where the voting system appears to record a vote as usual, while in reality, no vote is stored or processed when authentication occurs with a duress password [9].

Duress passwords have clear applications in intelligence and military contexts [9]. However, their use has not been systematically evaluated, nor has their application in civilian contexts been extensively studied, aside from limited exploration in the electronic voting domain [10, 13]. Other potential application areas include home security systems, ATMs, and database redirection under duress, as supported by existing patents [1, 21, 27]. Previous work has also proposed duress password solutions specifically for ATMs [17]. However, to the best of our knowledge, no study has investigated user perceptions of duress passwords, including their potential use cases. This research aims to address this research gap by answering the following research question: *How do users perceive the potential use cases of duress passwords?*

To answer this question, we conduct an online survey with 300 participants, in which the concept of duress password is explained to them, and they are asked an open-ended question about whether they can think of situations where using a system with duress passwords could be useful. To analyse the data, an open-coding approach is employed, with codes grouped into themes. Our findings show that users perceive critical systems handling sensitive data as use cases of duress passwords, given the potentially severe consequences of a duress attack. Furthermore, they consider duress passwords applicable to personal accounts, such as banking. Additionally, users perceive duress passwords as secure and usable, as they are harder to crack and easier to remember. Therefore, our findings emphasise the possible value of duress passwords for mitigating duress attacks in both critical systems and personal accounts.

2 Related work

A substantial number of studies have investigated how to improve the usability of passwords [2, 8, 22–24, 28]. In particular, the memorability of passwords has gained attention, as users tend to choose short, weak passwords that they reuse on multiple platforms [5, 14,

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

CSCW Companion '25, Bergen, Norway
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1480-1/2025/10
https://doi.org/10.1145/3715070.3749266

18]. However, none of these studies address the problem of duress upon authentication, which is the focus of this study.

2.1 Technical Solutions for Duress Attacks

Several technical solutions have been offered to address the issue of duress attacks [4, 13, 15–17, 31, 32]. Among these, biometric approaches have been explored. However, such approaches introduce privacy concerns due to the sensitive nature of biometric data [15, 16]. Another approach utilises implicit learning from cognitive psychology to plant a secret password in the user's brain without their conscious awareness, thereby making it resistant to forced disclosure by the user [4]. Yet, such an approach is accompanied by ethical considerations. Other techniques enable users to trigger deletion operations that either simulate normal behaviour or provide strong technical guarantees of erasure, even when inspected by an adversary [31, 32]. However, deletion operations might not be suitable for all contexts. Additionally, duress-resistant mechanisms have been proposed for specific use cases such as ATMs and electronic voting [10, 13, 17].

2.2 Dictionary-based Duress Password Schemes

Clark et al. [2008] introduced the concept of using dictionaries for duress detection. In their 5-dictionary scheme, a user's password consists of five words from a chosen dictionary designed to support three input types: (1) the valid password, which logs in successfully; (2) a duress password, formed by any other valid combination of five dictionary words, which appears to succeed but triggers hidden countermeasures; and (3) an invalid password, which results in a standard error. This approach is extended by Stefanov et al. [2010], who propose a simplified variant requiring users to memorise a single dictionary word in addition to their main password. During normal authentication, both are entered correctly. Under duress, the user supplies an alternative dictionary word as the covert signal. Inputs outside the dictionary are treated as invalid, making duress entries indistinguishable from legitimate ones to an adversary.

3 Methodology

To answer how usable users perceive duress passwords, we conducted an online survey using the Prolific platform [25]. The participants were randomly assigned to one of three duress password dictionaries [1]: *animals, countries, and colours.* The dictionaries were chosen because they are cognitively easy to apply, aligning with one of the key requirements of the duress password scheme proposed by Stefanov and Atallah [2010], which we follow in this study.

3.1 Survey Design

Participants were first welcomed and shown a consent form. Afterwards, we explained the concept of duress passwords to them. We referred to these as 'thematic passwords,' a less negative term used to avoid bias. To answer our research question, we asked participants an open-ended question about situations in which using a duress password could be useful. In addition, we asked them demographic questions [2]. Furthermore, our survey included an attention check for quality control, following Prolific recommendations [26]. To validate our questions and identify potential issues, we conducted a test session with a researcher present to observe and identify any issues, especially regarding the explanation of duress passwords. Furthermore, we conducted a pilot with 30 participants on Prolific.

3.2 Recruitment and Ethics

We recruited 300 participants through Prolific, all of whom were residents of the United Kingdom or the United States and fluent in English. We offered participants £8.97 in reimbursement for a study duration of 17.24 minutes, which is above the average payment on Prolific. While our institution does not require ethical review board approval, we followed the ethical guidelines of our institution, ensuring that the participants were able to provide informed consent about study participation and the collection of their data.

3.3 Data Analysis

We conducted open coding at the question level in Excel and used Miro to support a thematic analysis of the data. A researcher developed the initial codebook based on the first 100 answers. This was done by grouping similar responses, resulting in seven codes. The initial codebook was applied to the remaining answers, and when it was not sufficient to capture several answers, a new code was added. Afterwards, the researcher coded all the responses with the final codebook. To ensure some reliability, the researcher applied a code-recoding strategy with a week between the first and second coding of the data.

4 Results

A total of 281 participants were included in the data analysis after we excluded the participants who failed the attention check within the survey. Of them, 109 were male, 171 female, and one identified as non-binary. The most common age group was between 35 and 45 years old (77 out of 281).

In our analysis, we identified the following three themes for the use cases of duress passwords: personal accounts, high-risk users and institutional targets, and perceptions of security and usability.

4.1 Personal Accounts

Personal accounts encompass the following aspects: financial accounts and other personal accounts. This theme includes use cases related to personal accounts, which could benefit from having duress passwords implemented.

Financial accounts have been mentioned by 123 of our participants. This relates to platforms and tools used for storing, accessing, or transferring money. In particular, our participants consider online banking accounts to be a relevant use case. Besides online banking, other financial tools include PayPal, Apple Pay, and crypto wallets. P38 says: *"Could be very useful when logging into bank accounts on online platforms because it makes it more secure; if someone is forcing you to access the account and you use a different thematic*

[1] While the detailed comparison between the dictionaries is not the focus for answering the research questions with the current paper, we collected further data to enable such a comparison in future analyses, which is out of scope for this paper.

[2] Note that we also asked other questions, but the analyses of these are beyond the scope of this paper; hence, we omit them for the sake of brevity

password, the bank will freeze any transactions, and your money will be safe."

Other personal accounts is mentioned by 25 participants and includes relevant use cases for duress passwords such as email, social media, retail, and shared family accounts. P279 says: *"Parents can use theme words to limit access to certain things for kids. For example, “games” could unlock fun apps, and “school” could unlock learning tools."*

4.2 High-risk Users and Institutional targets

The theme encompasses the following aspects: vulnerable users and high-risk professions, and critical systems and institutional targets. This theme focus on use cases, which are relevant because the participants perceive some users and systems to be at higher risk of duress attacks.

Vulnerable users and high-risk professions are more prone to coercion, according to 18 of our participants. These professions include people employed in jobs that involve sensitive data, such as military personnel, journalists, and diplomats. Therefore, our participants perceive duress passwords to be a good use case for people in such jobs. P153 says: *"A journalist under threat uses a thematic password to access a sanitised version of their data while signalling they are under duress"*. Additionally, our participants perceive domestic abuse and kidnapped victims as relevant use cases, as these are more vulnerable to duress attacks.

Critical systems and institutional targets are relevant use cases for duress passwords, as the consequences of a successful duress attack are greater, according to 26 of our participants. In particular, this includes the military, hospitals, and governmental systems. P1 says: *"Financial institutions or critical infrastructure accounts, where unauthorised access could have serious consequences"*. Additionally, they perceive that work accounts should also apply duress passwords.

4.3 Perceptions on Security and Usability

Perceptions regarding security and usability do not relate as such to concrete use cases but instead elaborate on the security and usability aspects of duress passwords.

Perceptions of security are mentioned 83 times by our participants. Some participants believe duress passwords are irrelevant because everything is hackable. Others perceive the solution as secure because it is difficult to hack two passwords. P67 says: *"It would make it a lot harder for hackers to get into your accounts"*. Further, several perceive duress passwords as useful for two-factor authentication. P29 says: *"I think it could be useful for two-factor authentication, providing that little bit more security to confirm the identity of the user."*

Perceptions of usability are mentioned 19 times by our participants. In particular, several participants mention memorability, as they believe that it is easier to remember a password within a specific dictionary. P258 says: *"It can be useful to remember passwords easily"*. Additionally, one participant raises a concern about potential confusion before getting used to duress passwords. While another participant touches upon the fact that the user must be able to understand how and when to use the duress passwords. P156 says: *"The user needs to be able to understand how and when to use them and also the implications of using them"*.

4.4 Other

The following codes could not be grouped into any theme: context of device use, applicable to any system with passwords, general duress scenarios, and miscellaneous.

Context of device use is mentioned six times by our participants and focuses on whether a device is used in a public or private setting. Our participants perceive duress passwords as useful in public contexts, such as cafes, libraries, or public computers, where privacy is limited. P99 says: *"If you are in a public place with shared computers."*

Applicable to any system with passwords is mentioned by 13 participants, who consider duress passwords to be useful for all systems utilising passwords. P253 says: *"Anywhere you currently use passwords"*.

General duress scenario is mentioned by 13 participants and encompasses when our participants perceive duress passwords to be useful in any situation when someone is forced to log in without specifying the context. P93 says: *"Where someone is with you and being forced to log in under duress."*

Miscellaneous includes when our participants cannot find any use case for duress passwords. Furthermore, it includes answers that the researcher could not understand.

5 Discussion

High-risk Contexts for Duress Password Use. Our participants identified specific use cases where they consider duress passwords particularly applicable because of the potential consequences of a successful duress attack. In particular, they highlight systems with access to sensitive data, such as medical records or classified governmental data, where an attack can compromise confidentiality and potentially harm national security. Additionally, they highlight financial systems and banking accounts, where the consequence is a monetary loss. These identified use cases correspond with the real-world practices, as duress passwords are used by US government agencies [9, 29]. Moreover, duress passwords have been applied in some ATMs, and previous research has proposed a solution for implementing them in that context [17]. Further, all of these potential use cases also align with how the participants perceive that people in certain jobs are at higher risk of experiencing a duress attack (e.g., diplomats). Therefore, future studies should investigate how users employed in these high-risk jobs with access to systems with sensitive data (e.g., healthcare staff) perceive the concept of duress passwords. Furthermore, different application domains should be explored, as the use and perception of duress passwords may vary significantly across contexts. For example, hospital staff typically access systems multiple times per day to retrieve patient records, whereas military personnel might use such systems less frequently and under different threat models.

Acceptance of Duress Passwords. Even though our participants identify high-risk contexts as potential use cases, some participants believe that all accounts utilising passwords would benefit from implementing duress passwords, including their personal accounts (e.g., mail, social media, retail). This finding suggests that some users want stronger security for all accounts and are ready to adopt duress passwords generally. This perspective aligns with our finding that many participants responded to the questions about potential use cases by emphasising the added sense of security that duress passwords offer. Consequently, duress passwords could be a feature that brings reassurance and peace of mind to users across all systems that use passwords, and not just a niche solution for high-risk systems. Further, participants' perceptions of duress passwords as secure could positively affect their acceptance. Still, some participants are in general sceptical about the security of duress passwords, which is why such users might have a harder time accepting duress passwords. Consequently, future research should explore the underlying reasons why people would want to use duress passwords.

Our participants further perceive duress passwords as usable, as their valid duress password has a theme based on the chosen type of dictionary, which they consider easy to memorise. Consequently, duress passwords do not add a significant memorability burden compared to traditional authentication for users and therefore could be well-received by users if implemented — a critical factor, given that user acceptance is essential for the adoption of security mechanisms [3, 11, 12, 30]. However, the use of duress passwords presents challenges to users' mental models. Typically, users rely on password managers to store their passwords securely, but duress passwords cannot be stored due to their sensitive nature. Additionally, while conventional passwords are recommended to be complex random strings or passphrases, duress passwords can be simple dictionary words, which contradicts usual password security guidelines but is justified here since duress passwords function as secondary authentication. Moreover, standard systems provide immediate feedback when a wrong password is entered, allowing users to correct mistakes; in contrast, duress passwords do not trigger such feedback to avoid alerting potential attackers, which may increase cognitive load and affect memorability. Additionally, in the case of a coercion attack, the user needs to use the duress password in a stressful situation, requiring them to recall and input it accurately under pressure, an aspect that significantly differs from normal authentication scenarios and further complicates the mental model. Thus, users might find it difficult to effectively apply duress passwords in real-world scenarios. Therefore, future work should investigate whether users can remember and correctly use duress passwords, given that their mental model differs from that of normal password authentication.

Limitations. A limitation of our study is that one researcher conducted the analysis, affecting the reliability of the results. To address this problem, the researcher used the code-recode strategy. Our participants, furthermore, did not interact with a real system implementing duress passwords, potentially affecting their perceptions. Additionally, they are most probably unfamiliar with duress passwords, as they are not implemented in many digital systems in the real world. Therefore, their lack of experience may have influenced their perceptions. Lastly, our participants are more educated than the standard population, potentially affecting the results.

6 Conclusion

In this work, we investigated the potential use cases of duress passwords, an authentication method designed to resist duress attacks, via a survey of 281 participants. We conclude that users consider systems with access to sensitive or highly confidential data to benefit from implementing duress passwords, as the consequences of a successful duress attack could be severe. As such, our participants mention use cases in the financial domain (e.g., coerced transactions), among journalists or others working with sensitive data (e.g., forced data disclosure), and for domestic abuse victims. Therefore, a thorough investigation of these and other relevant use cases is needed, including designing ways a system should react in case a duress password is entered (e.g., freezing transactions, hiding most sensitive data, contacting the authorities). Further future work should focus on evaluating the usability and memorability of duress passwords and ways to support users in successfully using them.

Acknowledgments

The work reported in this paper was supported by Independent Research Fund Denmark, grant number 10.46540/2101-00006B

References

[1] Leemon C. Baird, M. E. Harmon, R. R. Young, and James E. Armstrong. 2004. Apparatus and method for authenticating access to a network resource. United States Patent US6732278B1. Filed October 5th., 2004, Issued April 6th,2005.

[2] Arezou Behfar, Hanieh Atashpanjeh, and Mahdi Nasrullah Al-Ameen. 2023. Can Password Meter be More Effective Towards User Attention, Engagement, and Attachment?: A Study of Metaphor-based Designs. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing (CSCW '23 Companion)*. ACM, Minneapolis, MN, USA, 1–8. doi:10.1145/3584931.3606983

[3] Saurav Bhattacharya, Sriram Panyam, Gaurav Deshmukh, Sudha Gatala, Vamsi Vemoori, and Dhruv Seth. 2024. Integrating User Experience and Acceptance in Authentication: A Synthesis of Technology Acceptance Model and User-Centered Design Principles. *International Journal of Computer Trends and Technology* 72, 4 (2024), 15–23. doi:10.14445/22312803/IJCTT-V72I4P102

[4] Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, and Patrick Lincoln. 2014. Neuroscience meets cryptography: crypto primitives secure against rubber hose attacks. *Commun. ACM* 57, 5 (May 2014), 110–118. doi:10.1145/2594445

[5] Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords . In *2012 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Los Alamitos, CA, USA, 538–552. doi:10.1109/SP.2012.49

[6] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy*. 553–567. doi:10.1109/SP.2012.44

[7] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2015. Passwords and the evolution of imperfect authentication. *Commun. ACM* 58, 7 (June 2015), 78–87. doi:10.1145/2699390

[8] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. 2009. Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '09)*. Association for Computing Machinery, New York, NY, USA, 500–511. doi:10.1145/1653662.1653722

[9] Jeremy Clark and Urs Hengartner. 2008. Panic passwords: Authenticating Under Duress. In *Proceedings of the 3rd Conference on Hot Topics in Security* (San Jose, CA) *(HOTSEC'08)*. USENIX Association, USA, Article 8, 6 pages.

[10] Jeremy Clark and Urs Hengartner. 2012. Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance. In *Financial Cryptography and Data Security*, George Danezis (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 47–61. doi:10.1007/978-3-642-27576-0_4

[11] Sanchari Das, Bingxing Wang, Zachary Tingle, and L. Jean Camp. 2019. Evaluating User Perception of Multi-Factor Authentication: A Systematic Review. In *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*. https://ssrn.com/abstract=3438207

[12] Fred D. Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* 13, 3 (Sept. 1989), 319–340. doi:10.2307/249008

[13] Alexander Essex, Jeremy Clark, and Urs Hengartner. 2012. Cobra: Toward Concurrent Ballot Authorization for Internet Voting. In *Proceedings of the 2012 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections* (Bellevue, WA) *(EVT/WOTE'12)*. USENIX Association, USA. https://www.usenix.org/conference/evtwote12/workshop-program/presentation/Essex

[14] Dinei Florencio and Cormac Herley. 2007. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web* (Banff, Alberta, Canada) *(WWW '07)*. Association for Computing Machinery, New York, NY, USA, 657–666. doi:10.1145/1242572.1242661

[15] Payas Gupta, Xuhua Ding, and Debin Gao. 2012. Coercion Resistance in Authentication Responsibility Shifting. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (Seoul, Korea) *(ASIACCS '12)*. Association for Computing Machinery, New York, NY, USA, 97–98. doi:10.1145/2414456.2414512

[16] Payas Gupta and Debin Gao. 2010. Fighting Coercion Attacks in Key Generation Using Skin Conductance. In *Proceedings of the 19th USENIX Conference on Security* (Washington, DC) *(USENIX Security'10)*. USENIX Association, USA, 30.

[17] Sufian Hameed, Syed Hussain, and Sohail Ali. 2013. SafePass: Authentication under duress for ATM transactions. In *Conference Proceedings - 2013 2nd National Conference on Information Assurance, NCIA 2013*. 1–5. doi:10.1109/NCIA.2013.6725317

[18] Ameya Hanamsagar, Simon S. Woo, Chris Kanich, and Jelena Mirkovic. 2018. Leveraging Semantic Transformation to Investigate Password Habits and Their Causes. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3173574.3174144

[19] Cormac Herley and Paul Van Oorschot. 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy* 10, 1 (2012), 28–36. doi:10.1109/MSP.2011.150

[20] Ari Juels, Dario Catalano, and Markus Jakobsson. 2010. *Coercion-Resistant Electronic Elections*. Springer Berlin Heidelberg, Berlin, Heidelberg, 37–63. doi:10.1007/978-3-642-12980-3_2

[21] R. J. Massa, T. R. Ellis, and R. G. LePage. 1986. Intelligent surveillance alarm system and method. United States Patent US4589081A. Filed March 15th., 1983, Issued May 13th, 1986.

[22] Naheem Noah, Peter Mayer, and Sanchari Das. 2023. A Proposal to Study Shoulder-Surfing Resistant Authentication for Augmented and Virtual Reality: Replication Study in the US. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing* (Minneapolis, MN, USA) *(CSCW '23 Companion)*. Association for Computing Machinery, New York, NY, USA, 317–322. doi:10.1145/3584931.3607007

[23] Rizu Paudel and Mahdi Nasrullah Al-Ameen. 2024. Leveraging the Power of Storytelling to Encourage and Empower Children towards Strong Passwords. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW2, Article 504 (Nov. 2024), 27 pages. doi:10.1145/3687043

[24] Rizu Paudel and Mahdi Nasrullah Al-Ameen. 2024. Priming through Persuasion: Towards Secure Password Behavior. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 110 (April 2024), 27 pages. doi:10.1145/3637387

[25] Prolific. 2025. Prolific Participant Recruitment Platform. https://www.prolific.com. Accessed: 2025-05-14.

[26] Prolific. 2025. Prolific's Attention and Comprehension Check Policy. https://researcher-help.prolific.com/en/article/fb63bb Accessed: 2025-05-15.

[27] R. K. Russikoff. 2005. Computerized password verification system and method for ATM transactions. United States Patent US6871288B1. Filed February 5th., 2004, Issued January 1st., 2005.

[28] Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. Correct Horse Battery Staple: Exploring the Usability of System-assigned Passphrases. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 7, 20 pages. doi:10.1145/2335356.2335366

[29] Emil Stefanov and Mikhail Atallah. 2010. Duress Detection for Authentication Attacks Against Multiple Administrators. In *Proceedings of the 2010 ACM Workshop on Insider Threats* (Chicago, Illinois, USA) *(Insider Threats '10)*. Association for Computing Machinery, New York, NY, USA, 37–46. doi:10.1145/1866886.1866895

[30] Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono. 2020. More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In *Proceedings of the 36th Annual Computer Security Applications Conference* (Austin, USA) *(ACSAC '20)*. Association for Computing Machinery, New York, NY, USA, 203–218. doi:10.1145/3427228.3427243

[31] Lianying Zhao and Mohammad Mannan. 2015. Gracewipe: Secure and Verifiable Deletion under Coercion. In *Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS)*. Internet Society, San Diego, CA, USA. https://www.ndss-symposium.org/wp-content/uploads/2017/09/04_2_2.pdf

[32] Lianying Zhao and Mohammad Mannan. 2016. Deceptive Deletion Triggers Under Coercion. *IEEE Transactions on Information Forensics and Security* 11, 12 (Dec. 2016), 2763–2776. doi:10.1109/TIFS.2016.2598523