Vision: What Johnny learns about Password Security from Videos posted on YouTube

MATHIEU CHRISTMANN, Technical University of Darmstadt, Germany
PETER MAYER and MELANIE VOLKAMER, SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology, Germany

The text password is the most pervasive authentication scheme and is unlikely to disappear soon. Companies employ password awareness and training campaigns to reduce the risk of insecure password management endangering these companies. While larger companies may buy measures for those campaigns externally or develop their own ones, small and medium-sized companies (SMEs) are likely to turn to freely available material – most likely videos – as they don't have budget and own experience to handle it like larger companies. We analysed such freely available videos and show their shortcomings. To that end, we aggregated requirements from the existing literature and applied these to a body of 32 freely available YouTube videos using search terms informed by Google Trends. The contributions of this work are two-fold. Firstly, the findings of our analysis show that the best video covers only about half of the requirements, which raises serious concerns regarding the quality of available videos and their suitability for usage in awareness campaigns by SMEs. Secondly, our list of aggregated requirements can inform the design of future videos, which is planned as a follow-up to this work to remedy the concerns uncovered in our analysis.

1 INTRODUCTION

Nowadays, people use an enormous and still growing number of applications, online services, and platforms. Most of them require the users to authenticate to get access. Text passwords are and will remain shortly the most common authentication scheme [8, 14]. At the same time, password attacks are the most frequent reasons for security incidents in companies [4, 10, 15, 19]. The estimated overall damage regarding cyber-attacks in Germany in 2019 was 102.9 billion euros [4]. One common way to address these issues is through awareness and training measures. In particular, small and medium sized companies (SMEs) are likely to refer their employees to available material on the Internet.

Our research aims to analyse the quality of freely available videos on YouTube, which try to raise awareness and educate users on secure passwords and secure password management. To do so, we first derived from literature a catalogue of 26 requirements for password security awareness and training measures. Afterwards, we conducted a structured search for relevant videos on YouTube in both German and English. A set of 32 videos was assessed according to our catalogue. Unfortunately, the best performing video only met 16 of our 26 requirements. This finding is alarming: companies and users alike might feel secure when following the advice from such videos, while the videos de facto contain information that is not up-to-date or even miss essential information completely. In discussing our findings, we

Table 1. Overview of evaluation requirements (G.1-E.1 are taken from [12, 13])

Category	ID	Source	Description
			Content Requirements
General	G.1	M1 [13]	Attackers are not only criminal hackers but also people you know.
General	G.2	M2 [13]	People believe that they are not important enough to be targeted by an attacker.
General	G.3	M3 [13]	Security requirements do not depend on how often the service is used.
General	G.4	M4 [13]	Security is not only the responsibility of the IT department.
Creation	C.1	A7 [12]	Targeted guessing
Creation	C.2	A8 [12]	Unspecified guessing
Creation	C.3	M12 [13]	The attacker can automate attack A8.
Creation	C.4	M13 [13]	Keyboard patterns are not secure passwords (even if they contain special characters and numbers).
Creation	C.5	M14 [13]	Attackers adapt the word lists to the attack targets.
Creation	C.6	M16 [13]	Passwords are not automatically more secure by special characters as well as numbers and must be as long as possible.
Creation	C.7	M17 [13]	Software automatically concatenates single entries of the word list and mimics human behaviour.
Creation	C.8	M18 [13]	Birth dates do not make passwords more secure either.
Creation	C.9	M20 [13]	Prefer a long password of letters to a short password of all character categories.
Management	M.1	A2 [12]	Stealing an insecurely stored note
Management	M.2	M6 [13]	Write down passwords in the beginning until you know them by heart instead of reusing passwords.
Management	M.3	M19 [13]	Changing passwords as a precaution does not increase security. The password should only be changed in case of an incident.
Management	M.4	M21 [13]	Even strong passwords should not be reused.
Management	M.5	A10 [12]	Stealing unencrypted electronic notes
Entering	E.1	A3 [12]	Shoulder surfing
			Design Requirements
Design	I.1	[12, 18, 22]	Identify risks and consequences, then describe the solution.
Design	I.2	[1, 2, 7, 11, 12, 17, 20, 21]	Motivate for strong passwords (e.g., by explaining the goal of the training).
Design	I.3	[5]	Use self-reflection.
Design	I.4	[7, 16]	Tell about all costs and benefits directly mapped to the user.
Design	I.5	[2, 12]	Easy to understand
Design	I.6	[2, 12]	Plausible and applicable to the reality of the user
Design	I.7	[3, 14, 21, 23]	Indicate that recommendations may not match the user's perception.

conclude that it is important to raise awareness about the general drawbacks of these videos and that – as a consequence – one should be careful when using freely available and untested material in awareness and training campaigns.

2 REQUIREMENTS

To conduct our analysis of freely available videos on YouTube which try to raise awareness and educate users on secure passwords and secure password management, we aggregated from literature requirements based on which awareness measures should be assessed. These belong to two categories: content and design requirements. While explicit

descriptions of all requirements are beyond the scope of this paper due to space constraints, a list of all requirements is provided as an overview in Table 1.

For the content requirements, we looked at literature outlining content users should know regarding authentication in general and selecting secure text passwords in particular. Mayer et al. [12, 13] provide a comprehensive list of such content based on reviews of the research literature. They present a list of misconceptions [13] that should be addressed as well as a list of attacks and counter-strategies [12] of which users should be aware. Note that not all of their misconceptions and attacks were deemed relevant in the context of this work since they are not related to selecting secure text passwords.

There is a similarly large body of literature on how to best design (security) education materials for the design requirements. From these, we derived the design requirements which password education materials should meet. For example, the audience should be motivated for strong passwords in the beginning by explaining the goal of the education measure (I.2) [1, 2, 7, 11, 12, 17, 20, 21]. Another critical requirement is to tell the audience that the learning content may not match their perception (I.7) because they may have outdated information [3, 14, 21, 23]. All design requirements are meant to ensure that the education material is as effective as possible and to deliver a good learning experience.

3 EXPLANATORY VIDEOS

3.1 Identifying a List of Videos to be Assessed

Existing videos were searched on YouTube because this is the leading platform for videos, according to [9]. Relevant search terms were identified using Google Trends[1] with the following settings:

- **Location:** "Germany" for German keywords; "Worldwide" for English keywords
- **Time Period:** 12 months
- **Category:** All Categories
- **Scope:** YouTube search

The search terms listed in the following were examined using Google Trends to determine how common they were on YouTube. Since the volume of the keywords mentioned above (in particular for "Secure Passwords", "Strong Passwords" and "Sichere Passwörter") was relatively low, the keywords "Passwords" and "Passwörter" were added to make sure that there was no crucial existing video missed in the analysis.[2]

- **German** "Sichere Passwörter" / **English** "Secure Passwords" / **English** "Strong Passwords"[3]
- **German** "Passwortsicherheit" / **English** "Password Security"
- **German** "Passwörter" / **English** "Passwords"

Based on the list of three German and four English search terms, a search on YouTube was performed[4] to identify explanatory videos about password security for our analysis. Each keyword was searched using a new instance of Google Chrome's incognito mode to eliminate bias from the previous searches. The localisation of the YouTube search was set to "DE-DE" for the German search terms and to "US-EN" for English search terms. The search results were sorted by relevance and filtered to include only videos which are no longer than 10 minutes according to the proposal of short-term training by Herley [7]. For each search term, the first 10 results were considered in our analysis.

[1] https://trends.google.com/trends/
[2] "Passwords" had a 200% higher search volume compared to "Password Security".
[3] Since in English, the usage of "secure" and "strong" passwords is common, both keywords are used.
[4] The search was performed on 11/10/2020.

Consequently, based on the 7 search terms, 70 videos were examined[5] in total. However, during a first screening, only 32 out of 70 videos were found to be in the scope for our analysis. The remaining 38 videos were found to be out of scope, each for one of the following reasons: (a) the video was about another topic (e.g., password managers, hashing, brute force software); (b) the video was not an explanatory video, e.g., a satirical contribution; (c) the video was already found using a previous search term. The complete list of assessed videos is due to space constraints provided digitally here.

3.2 Assessment of Existing Explanatory Videos

Each of the 32 videos in-scope was watched and its content matched against the content and design requirements listed in Table 1. The coverage rate is calculated using the following formula:

$$\textbf{CoverageRate} = \frac{\#CoveredRequirements + \frac{\#PartiallyCoveredRequirements}{2}}{\#AllRequirements}$$

The aggregated assessment results of each video are shown in Figure 1. According to the calculated coverage rate, video "EN-1A-07" (from Linus Tech Tips on Password Security Best Practices [6]) performs best in our analysis. Still, with a coverage rate of only 57.7%, the video fails to cover nearly half of all requirements. The best performing German video is DE-1-08 from Simplicissimus[7], with a coverage rate of 55.8%.

On average, the assessed videos cover only 26.1% of the requirements, which is relatively low. When looking at the differences between English (27.1%) and German (24.9%) videos, only a tiny difference appears. An aggregated overview of the fulfilment per each requirement is shown clustered by attacks in Figure 2, by misconceptions in Figure 3 and by design requirements in Figure 4. The requirements fulfilled most frequently are:

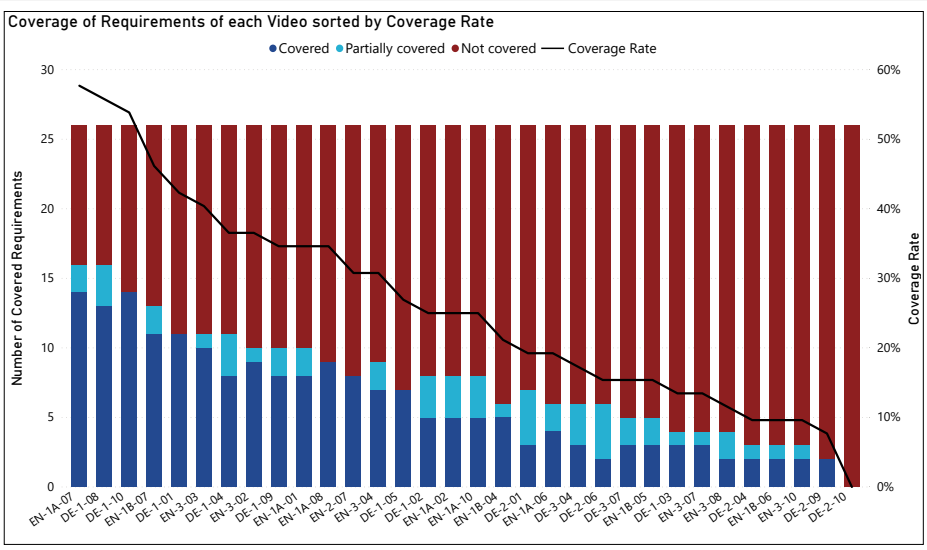

Fig. 1. Number of covered, partially covered and not covered requirements as well as coverage rate for each assessed video.

[5] Between 11/11/2020 and 11/21/2020
[6] https://www.youtube.com/watch?v=t8SQo3R7qeU
[7] https://www.youtube.com/watch?v=qR7xFprYnF0

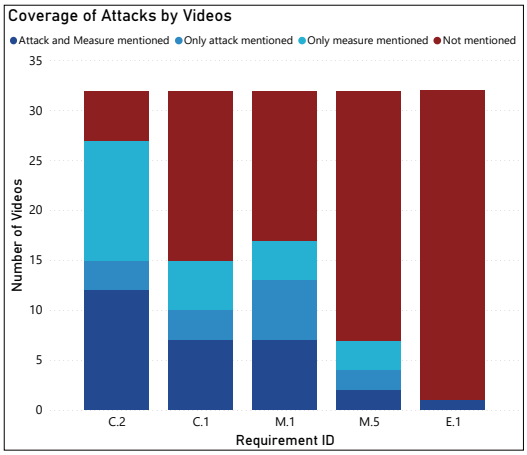

Fig. 2. All requirements, which are **attacks**, and their cover-

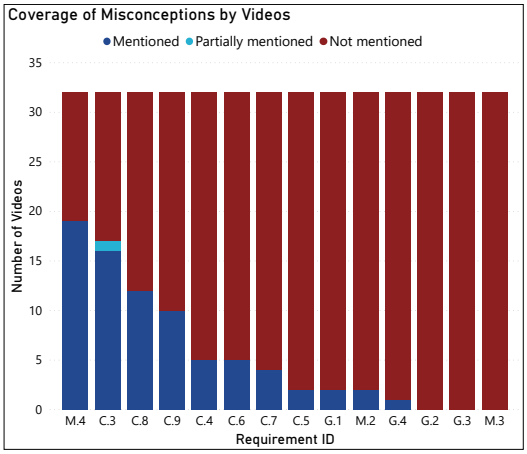

Fig. 3. All requirements, which are **misconceptions**, and their coverage rate of the assessed videos.

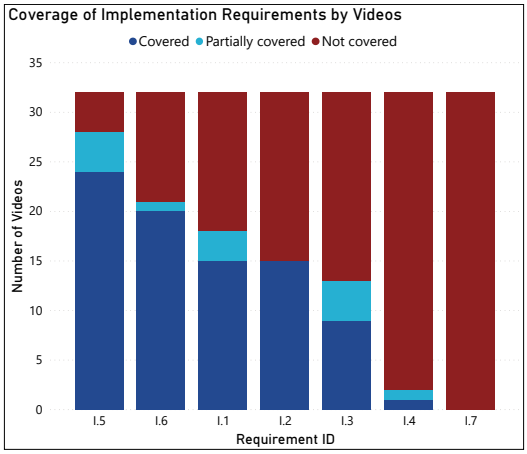

Fig. 4. All **design** requirements and their coverage rate of the assessed videos.

- C.3: The attacker can automate attack A8 (while A8 is: Unspecified Guessing).
- C.8: Birth dates do not make passwords more secure either.
- C.9: Prefer a long password of letters to a short password of all character categories.
- I.5: Easy to understand
- I.6: Plausible and applicable to the reality of the user

However, there are also a lot of requirements, which are hardly covered, e.g.:

- G.1: Attackers are not only criminal hackers but also people you know.
- C.4: Keyboard patterns are not secure passwords (even if they contain special characters and numbers).
- C.6: Passwords are not automatically more secure by special characters as well as numbers and must be as long as possible.

- M.2: Write down passwords in the beginning until you know them by heart instead of reusing passwords.
- I.4: Tell about all costs and benefits directly mapped to the user.

There are even requirements that are not covered at all, e.g.:

- G.2: People believe that they are not important enough to be targeted by an attacker.
- G.3: Security requirements do not depend on how often the service is used.
- M.3: Changing passwords as a precaution does not increase security. The password should only be changed in case of an incident.
- I.7: Indicate that recommendations may not match the user's perception.

The detailed assessment results of each video cannot be provided here due to space constraints but are instead digitally available here. The table shows the results of each video according to the content and design requirements. Additionally, a column "Remark" for further information on the assessment is included, such as a reason for excluding the video of the assessment, giving reference to its duplicate, or if there is a particular memory strategy is proposed.

4 DISCUSSION

We assessed 70 videos on password security which we found using a structured search on YouTube. 32 of these were analysed in detail. We used requirements which we aggregated from the literature to assess all 32 videos. In our analysis, we found that none of the existing videos fulfil all requirements. The best one covers only about half the requirements. Therefore, serious concerns regarding their suitability for awareness campaigns arise. It seems none of them can be genuinely recommended to be used in such campaigns – especially if the video is the only resource provided to the employees.

In particular, several misconceptions identified in [13] are not or rarely addressed by these videos. The most critical ones are (a) that patterns or walks on the keyboard should not be used and (b) that the security requirements of a password do not depend on the frequency of use of the respective account but instead depend on the data and action accessible in that account. Furthermore, governmental authorities such as NIST, the German BSI, and the UK NCSC recommend not to use password expiration. However, this is not at all reflected in the assessed videos. Some videos explicitly include this outdated recommendation to change the passwords pro-actively.

Overall, we argue that using such videos can be dangerous. Users may feel a false sense of security after watching the videos, while the advice might be indeed incomplete or outdated. Therefore, we believe that our list of requirements should guide the development and design of future awareness videos on password security. Consequently, we started developing a password awareness video fulfilling all the identified requirements. A description of the video content, the video itself, as well as a very first evaluation are available in [6] (at 2021 WAY@SOUPS workshop).

Furthermore, especially in the business context, it is vital to cover all identified requirements to truly enable users to protect themselves and reduce the risks to businesses. Our aggregated list of requirements can be used, e.g., by CISOs of SMEs, to assess any videos (and potentially other awareness material as well) they intend to use in their awareness campaigns. Suppose the coverage rate of the requirements is low. In that case, videos should be improved (if that is an option open to the CISO); otherwise, it might be better to forego the existing videos entirely.

ACKNOWLEDGMENTS

This research was supported by the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS).

REFERENCES

[1] Anne Adams and Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42 (12 1999), 40–46. https://doi.org/10.1145/322796.322806

[2] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? arXiv:1901.02672 [cs.CR]

[3] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2018. The rewards and costs of stronger passwords in a university: Linking password lifetime to strength. *Proceedings of the 27th USENIX Security Symposium* (2018), 239–253.

[4] Bitkom. [n. d.]. *Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr.* https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr.

[5] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 2019. 23 Ways to Nudge: A review of technology-mediated nudging in human-computer interaction. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300733

[6] Mathieu Christmann, Peter Mayer, and Melanie Volkamer. 2021. How to Effectively Communicate Benefits of Introducing a Modern Password Policy to Employees in Companies. In *Who Are You?! Adventures in Authentication Workshop (WAY '21)*. Virtual Conference, 1–7.

[7] Cormac Herley. 2009. So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings New Security Paradigms Workshop* (2009), 133–144. https://doi.org/10.1145/1719030.1719050

[8] Cormac Herley and Paul Van Oorschot. 2012. A research agenda acknowledging the persistence of passwords. *IEEE Security and Privacy* 10, 1 (2012), 28–36. https://doi.org/10.1109/MSP.2011.150

[9] Alexa Internet. [n. d.]. *Keyword Research, Competitive Analysis & Website Ranking | Alexa.* https://www.alexa.com/.

[10] Anthony Jameson, Silvia Gabrieli, Per Ola Kristensson, Katharina Reinecke, Federica Cena, Cristina Gena, and Fabiana Vernero. 2011. How can we support users' preferential choice? *Conference on Human Factors in Computing Systems - Proceedings* (2011), 409–418. https://doi.org/10.1145/1979742.1979620

[11] C. Lin and A.S. Kunnathur. 2013. Toward developing a theory of end user information security competence. *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime* 5 (01 2013), 3578–3587.

[12] Peter Mayer, Christian Schwartz, and Melanie Volkamer. 2018. On The Systematic Development and Evaluation Of Password Security Awareness-Raising Materials. In *Annual Computer Security Applications Conference*. ACM, 733–748. https://doi.org/10.1145/3274694.3274747

[13] Peter Mayer and Melanie Volkamer. 2018. Addressing Misconceptions about Password Security Effectively. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust* (Orlando, Florida, USA) *(STAST '17)*. Association for Computing Machinery, New York, NY, USA, 16–27. https://doi.org/10.1145/3167996.3167998

[14] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. 2013. Measuring password guessability for an entire university. *Proceedings of the ACM Conference on Computer and Communications Security* (2013), 173–186. https://doi.org/10.1145/2508859.2516726

[15] Harri Oinas-Kukkonen and Marja Harjumaa. 2009. Persuasive systems design: Key issues, process model, and system features. *Communications of the Association for Information Systems* 24, 1 (2009), 485–500. https://doi.org/10.17705/1cais.02428

[16] Karen Renaud and Verena Zimmermann. 2019. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy* (2019). https://doi.org/10.1017/bpp.2018.3

[17] Stefan Stieglitz, Tobias Potthoff, and Tobias Kißmer. 2017. Digital Nudging am Arbeitsplatz. *HMD Praxis der Wirtschaftsinformatik* (2017). https://doi.org/10.1365/s40702-017-0367-5

[18] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 123–140. https://www.usenix.org/conference/soups2015/proceedings/presentation/ur

[19] Verizon. 2020. *Verizon 2020 Data Breach Investigations Report.* Technical Report. Verison.

[20] Melanie Volkamer and Benjamin Bachmann. [n. d.]. *Wie Sie Ihre Mitarbeiter für IT-Sicherheit sensibilisieren.* https://www.verwaltung-der-zukunft.org/oeffentliche-it/wie-sie-ihre-mitarbeiter-fuer-it-sicherheit-sensibilisieren.

[21] M. Yıldırım and I. Mackie. 2019. Encouraging users to improve password security and memorability. *International Journal of Information Security* (2019). https://doi.org/10.1007/s10207-019-00429-y

[22] Nur Haryani Zakaria. 2013. Exploring human factors issues & possible countermeasures in password authentication.

[23] Leah Zhang-Kennedy, Sonia Chiasson, and P Oorschot. 2016. Revisiting Password Rules: Facilitating Human Management of Passwords. https://doi.org/10.1109/ECRIME.2016.7487945