How well do young adults understand their online security? A study on password practices and safeguard implementation.

Author: Abdulla AlBassam

ABSTRACT

Data breaches and leaked credentials are becoming increasingly common, with an alarming number of weak or reused passwords found on the internet (Verizon, 2021; LastPass, 2021). Although cybersecurity professionals advocate for unique and stronger credentials, many users, particularly in terms of this study young adults, still choose convenience and ease over robust security measures. This study explores password habits among 18–25-year-olds across diverse educational backgrounds, focusing on key issues such as password reuse, the adoption of two-factor authentication (2FA), and attitudes toward auto-generated passwords. Using in-depth, open-ended interviews, we uncover how perceived "low risk," lack of awareness, and security apathy undermine safer practices. Despite acknowledging potential threats, participants often reuse a small set of credentials and express mistrust of password managers, citing memorability concerns or "hassle." These findings underline the gap between being knowledgeable and taking action, emphasizing the need for targeted interventions beyond just general awareness campaigns to address the ingrained convenience-over-safety mentality in younger demographics.

Additional Keywords and Phrases: Passwords, Interviews, Cybersecurity habits, Two-Factor Authentication.

INTRODUCTION

In 2024, an unprecedented leak on "breach forums" exposed nearly 10 billion passwords (winder, 2024). Despite urgent warnings from cybersecurity experts, many individuals still reuse weak credentials or neglect safeguards such as Two-factor authentication (2FA). Research confirms that stolen or reused passwords account for the majority of breaches (Verizon, 2021; LastPass, 2021). Because young adults drive much of our online world, building robust cybersecurity habits in this demographic is critical for preventing future large-scale compromises, asking the question, how well do young adults understand their online security?

BACKGROUND

PASSWORD REUSE AND "LOW-RISK" PERCEPTION

Password reuse is often rationalized by convenience. Existing literature details that when users perceive themselves as unlikely targets, they adopt minimal changes in their security behaviors, despite awareness campaigns (Ur et al., 2016; Madden et al., 2013). For young adults, this "low risk" perception may be an even bigger factor. Raised in an era of constant online interaction, they frequently juggle numerous accounts with similar or identical credentials, prioritizing memorability over security (Wash, 2010). This tension between convenience and risk further explains why repeated warnings about data breaches often fail to evoke action (Furnell, 2020).

TWO-FACTOR AUTHENTICATION (2FA) ADOPTION

Two-factor authentication (2FA) provides an additional layer of security by requiring a secondary verification method (NCSC, 2023). Studies show that 2FA significantly reduces the risk of unauthorized access (Das et al., 2014). However, users frequently cite "hassle" and "wasted time" as barriers (Ion et al., 2015). Among young adults, use of 2FA tends to be mixed, some use it for high-risk accounts (e.g. banking), while others avoid it altogether unless forced (Madden et al., 2013). This underscores the ongoing struggle between a desire for privacy and the convenience of simple passwords.

ATTITUDES TOWARD AUTO-GENERATED PASSWORDS

Auto-generated credentials offer randomness and security but spark user concerns about memorization and potential "lockouts" (Das et al., 2014). While some young adults acknowledge these benefits, they often pick shorter, easily memorized passwords (Mazurek et al., 2013).

YOUNG ADULTS' UNDERREPRESENTATION

Much of the existing literature on internet safeguard habits explores password behaviour in general populations or among those in the workforce (Furnell, 2020; Shay et al., 2014). However, young adults who have grown up in today's internet dependent age are often underrepresented in these studies. One might assume that early and constant exposure to the internet leads to more secure online habits, yet research indicates the opposite (Wash, 2010). While older generations may also rely on simpler passwords or overlook how data breaches compromise aspects of their lives (Ur et al., 2016), young adults' approach to security often reflects a tension between their desire for both privacy and convenience, which may not always coincide (Wash, 2010).

RATIONALE

By focusing on young adults' real-world experiences, this study addresses a gap in understanding the reasons behind their password choices and broader security decisions, namely why convenience and perceived "low risk" might undermine basic safety practices. Through interviews with 18–25-year-olds across diverse educational backgrounds (see justification), we aim to build upon the existing literature and highlight the motivations and barriers shaping personal cybersecurity habits.

METHOD

DESIGN

Through in-depth, open-ended questions, interviews were conducted with the aim to uncover how effectively these participants understand issues such as password reuse, the role of two-factor authentication, and best practices for strong password creation. By doing so, this research sheds light on the motivations, barriers, and potential misconceptions that shape personal online security choices within this age range.

PARTICIPANTS

For this qualitative study, the goal was to avoid interviewing people from the same background, as well as avoiding interviewing cybersecurity students only (see justification). I instead selected friends and colleagues, who's ages range between 18-25 that all study vastly different things to see the perspective of a more general population instead of focusing only on people with a background in cybersecurity studies. (see justification).

MATERIALS

An interview script (see justification).

PROCEDURE

8 of the interviews were conducted in person, and 3 were conducted on either Google Meets or Microsoft Teams, depending on the participants preference. All the interviews were recorded using the 'voice memo' app on iPhone. At the beginning of every interview, the interviewee was asked to rate how safe they believe their information is online on a scale of 1-10, and what they believe their level of comfort navigating technology is. (see justification) The rest of the questions centered around their password habits, how they remember/store their passwords (do they memorize, use a password manager, other…), if they have ever had an account or password compromised and what they did in response, if their password creation habits differ based on how sensitive they perceive that account to be (bank vs throwaway accounts) whether they employ 2FA and their opinions about it, whether they use autogenerated passwords and their feelings about them as compared to creating their own passwords, and a final general question about their experiences with online scams, to use as a comparison to see how they react to scams vs password/data leaks.

ANALYSIS

Two central themes emerged from the interviews: the ongoing tension between convenience and safety, and a lack of knowledge or awareness regarding safeguards like 2FA and auto-generated passwords.

CONVENIENCE OVER SAFETY

This was by far the most common theme. Although easy-to-remember passwords and bypassing safeguards saves time, these practices leave accounts vulnerable. When asked why they reuse passwords, **P1** stated that it's

"…because I want to remember all the passwords, so I just use five." All 11 interviewees admitted to reusing passwords at least once, with **P4** and **P6** being the worst offenders. They reported "three or four" passwords and just two passwords across 100+ accounts, respectively. **P5** (15 passwords) and **P7** (24) also reuse them, though to a lesser degree. Five participants mentioned data leaks or compromise notifications; **two** (P1, P9) took no action. In one exchange:

Interviewer: "Have you ever been told one of your passwords has been compromised?"
P9: "Yes."
Interviewer: "What was your experience?"
P9: "I didn't do anything about it."

P1 and P9 share a common "not worth the hassle" outlook, while P2, P5, and P8 only reacted if they felt a real threat. None claimed to change passwords proactively.
Regarding 2FA, six participants (P2, P5, P6, P7, P8, P10) were open to using it in some capacity, and the others (P1, P3, P4, P9, P11) would avoid it unless forced. When asked if they would use 2FA all the time, only **P7** said yes. Others found it frustrating:

P5: "Oh, it'd be too much of a hindrance…too long."
P9: "I don't think [2FA] is helpful or necessary… I complain about it all the time. I would like to stop using it."
P11: "It's too annoying."

Similarly, only three participants said they would use auto-generated passwords or preferred them over their own. While some acknowledged their benefit, they still felt memorizing their own passwords was easier:
P3: "Because they're always really complicated. I'm never gonna remember them."
P11: "no, never. It's too, like, weird, too long… I would want to remember it myself."

LACK OF AWARENESS

Many participants showed security apathy and/or limited awareness about available safeguards, even when they recognized potential risks. Indifference toward proactive measures and a mixed understanding of key concepts, especially 2FA and auto-generated passwords, surfaced in their statements.

2FA KNOWLEDGE GAPS

Several participants misunderstood or didn't realize they were already using 2FA. For example:

P4: "Uhh, I don't know."
Interviewer: "So you wouldn't say you've ever used it before?"
P4: "probably… oh yeah, duo push for uni. I didn't know that was 2FA."

P6 stated:
"I don't really know what that is… is that when they send you something, like a code?"

AUTO-GENERATED PASSWORDS

A similar lack of clarity arose around password managers. For instance:

P3: “because they’re always really complicated. I’m never gonna remember them.”
Interviewer: “did you know [autogenerated passwords] are stored locally on your device?”
P3: “No.”

P4 asked:
“No… they’re too long. And I’m like, if I save it, will it actually be saved?”

P10 commented:
“i use auto-generated passwords for, like, games or social media, but not for banking… I’d rather memorize my own for critical accounts.”

These quotes detail concerns about reliability and a tendency to favour convenience over robust security measures.

DISCUSSION

The most glaring aspect of these findings is the tension between convenience and security. Although it may seem logical that early internet exposure would translate to stronger safeguards, participants repeatedly cited the ease of memorising passwords, and perceived low risk of their data to justify password reuse or neglect of features like 2FA. These attitudes confirm the theme identified by Wash (2010), who noted that viewing data breaches as “unlikely” leads to security apathy. Furthermore, this highlights Furnell’s (2020) observation that users often fail to employ stronger defence measures despite awareness campaigns. (See justification)

Another noteworthy outcome is the lack of awareness regarding critical tools, such as auto-generated passwords and how they can be securely managed across devices. Several participants expressed concerns about “not remembering complex passwords” or “not knowing if they’re actually saved.” This aligns with prior studies (Ur et al., 2012; Das et al., 2014) indicating users’ mistrust of password managers. Even those who recognized the benefits of auto-generated credentials, such as P10, often opted against high-security logins, preferring personal memorization to an external system, displaying the “partial adoption” phenomenon discussed by Wash (2010).

These findings also reinforce Shay et al. (2014) and LastPass (2021) conclusions that while many individuals are aware of what safe cybersecurity behaviours are, only few translate that knowledge into action. This underscores the need for educational interventions, not just general reminders about password strength, but practical demonstrations of how tools like 2FA and autogenerated passwords actually work and why they matter.

Overall, these results enrich the existing bodies of work by pinpointing where user knowledge breaks down and how security apathy persists despite awareness. By clarifying that even young adults demonstrate negative security habits, this study provides a basis for further research into designing more robust solutions that can resonate with convenience focused people.

REFLECTION

In reflection of the research conducted, both in terms of the interviews conducted and the paper writing aspect, there was room for improvement. I leaned towards 1 on 1 interviews because they seemed to be the best option for my research topic. It ensured I could get as non-bias of answers as possible, due to the fact that I had full control on who participated (as opposed to surveys). I believe that some of the interviews were better than others, both in terms of my performance and in the quality of answers from the participants. I would like to believe that my questions were open-ended enough to warrant explanations and provoke some deep thinking and some self-reflection on their password habits and general attitude towards their online safety. However, after analyzing/coding the data, I realized that some participants' answers could have been more elaborate, and that I should have done a better job in extracting those answers out of the participants. I learned that it is my job to continue asking questions until I believe the answer to be sufficient, participants won't always be so forthcoming. I realized that I was sometimes quick to jump to the next question, mainly in the first few interviews. In self-reflection, I seemed unconfident during the start of the interview process, a little shy to delve deeper into the why's and how's the participant does something. I gained more confidence and had more vigorous questioning in the latter half of my interview process, though.

In future work, I will ensure I have a rough idea of the main topics I would want to cover on the actual paper, so that I can leave out some fluff from the interviews. I overestimated the word count of the paper itself, not realized how restricting 1,500 words really were, because of that, I feel like I left out a lot of key info that could have made my paper much stronger than it is. In fact, this was unexpectedly the most challenging part of the whole assignment. I had conducted 11 interviews, ranging from 5-10 mins which contained so much information that I would have loved to include. Because of this, condensing the paper down to the 1500 words was stressful, complicated, and even at the end, I am unsure if what I chose to leave on the cutting board were the best, strongest, points. Although, this did teach me that condensing information is key, and focusing on the "nitty gritty" is what matters in drawing robust conclusions. In light of this, in future work, I'll make sure to start on the paper earlier than when I did, giving me time to ask questions in class, discuss with peers, and ensure that the content in the paper is the strongest it could be.

The recruiting process was not too bad, and neither were the actual interviews, bar issues mentioned above, and having to chase the participants to sign the ethics form, which looking back, I should have obviously had them sign before the interview process, instead of emailing it to them and giving them all the time in the world to get to signing it. The coding aspect, while tedious, was essential in helping build my knowledge on the interview content and be able to write the actual paper.

I regret not including some questions, mainly about biometrics, such as Face ID and fingerprints. This is a topic that was not touched on in other research papers covering similar topics and I believe it could have provided my paper with some depth that other similar papers to mine did not have. I realized halfway through my interview process that I did not touch on this subject at all, but at that point I believed it was too late to course correct. I did not want to begin asking these questions at that point, because then the sample size would not be nearly enough as compared to the rest of the questions. Speaking of past literature, there were a couple sources I had found in early December that were key, namely a paper by Kennedy et al., 2021, however when the deadline came closer, I could not find this paper anywhere. I still have no idea why, maybe I am mistaken, but it was the strongest, most similar paper to mine, I had found online and would have come

in handy in writing my paper, but because I couldn't find it when I was citing my sources, I had to unfortunately leave it out, and instead used slightly weaker, older, papers in its place. This could have been something I could have asked for help with, but due to starting the paper late, I was unable to.

Conducting interviews and writing research paper, as with everything in life, takes practice to perfect, and I will ensure to apply everything I learned during this process in any similar future work.

REFERENCES

[1] M. Madden, A. Lenhart, M. Duggan, S. Cortesi, and U. Gasser. 2013. *Teens and technology 2013.* Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2013/03/13/teens-and-technology-2013/

[2] B. Ur, P. G. Kelley, S. Komanduri, A. J. Lee, M. Maass, M. L. Mazurek, and L. F. Cranor. 2012. How does your password measure up? The effect of strength meters on password creation. In *Proceedings of the 21st USENIX Security Symposium (USENIX Security'12)*. USENIX Association, Bellevue, WA, 65–80.

[3] S. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. 2014. The tangled web of password reuse. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'14)*. Internet Society, San Diego, CA, USA. https://doi.org/10.14722/ndss.2014.23263

[4] Norton. 2022. Password statistics: The bad habits of password reuse. Retrieved from https://us.norton.com/blog/privacy/password-statistics

[5] R. Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS'10)*. ACM, New York, NY, 1–16. https://doi.org/10.1145/1837110.1837125

[6] M. L. Mazurek, S. Komanduri, T. Vidas, M. K. Reiter, L. Bauer, N. Christin, and L. F. Cranor. 2013. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS'13)*. ACM, New York, NY, 173–186. https://doi.org/10.1145/2508859.2516737

[7] I. Ion, R. Reeder, and S. Consolvo. 2015. "No one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS'15)*. USENIX Association, Ottawa, Canada, 1–20.

[8] S. Furnell. 2020. Cybersecurity in society: Privacy, ethics, and the need for user-centric approaches. *Computer Fraud & Security*, 2020(7), 11–17. https://doi.org/10.1016/S1361-3723(20)30072-1

[9] Verizon. 2021. *2021 Data Breach Investigations Report*. Retrieved from https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

[10] D. Winder. 2024. New security alert: Hacker uploads 10 billion stolen passwords to crime forum. *Forbes.* Retrieved from https://www.forbes.com/sites/daveywinder/2024/07/05/new-security-alert-hacker-uploads-10-billion-stolen-passwords-to-crime-forum/

[11] R. Shay, S. Komanduri, P. G. Kelley, P. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. 2014. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS'14)*. USENIX Association, Menlo Park, CA, 1–20.