Use of and Concerns about Online Authentication Technologies among British University Staff and Students

Ibtihal Alotaibi
University of York
York, United Kingdom[1]
ia893@york.ac.uk

Helen Petrie
University of York
York, United Kingdom
helen.petrie@york.ac.uk

Siamak F. Shahandashti
University of York
York, United Kingdom
siamak.shahandashti@york.ac.uk

Online services are now an essential part of everyday life, with most people having many online accounts. Staff and students at universities have much important information online which needs to be secure. The technologies used for authentication of online accounts as now grown from passwords to a range of different technologies including two-factor authentication (2FA), single sign on (SSO), biometric authentication (most often face or fingerprint recognition), Federated Identity Management (FIM), and Fast Identity Online (FIDO). Research has shown usability issues and user concerns about these technologies. An online survey was undertaken to investigate current levels of use and concerns about seven authentication technologies among British university staff and students. A wide range of technologies was used with passwords still being the most frequently used. Participants' ratings of ease of use, trust, perception of security and confidence in using the technologies was generally high, and ratings of concerns were low. There were interesting differences between the staff and student samples.

Authentication technologies. Use of authentication technologies. Authentication technologies concerns.. Passwords. Passcodes. Two factor authentication (2FA). Single Sign-On Authentication (SSO). Fingerprint authentication. Face recognition authentication. Fast Identity Online authentication (FIDO).

1. INTRODUCTION

Having all kinds of personal information, from the mundane to the sensitive, online has now become a normal part of everyday life. Most people have numerous online accounts with information that needs to be protected, from bank accounts to social media accounts with personal photos. Staff and students at universities have much of their professional and educational material online now, including student records, research and teaching materials, assignments and notes.

Online accounts are generally protected by users authenticating themselves, e.g. with usernames and passwords, although very sensitive accounts such as banking, often had more complex security measures. There are now a wide range of authentication technologies, in addition to the continued widespread use of passwords, including two-factor authentication (2FA), single sign on (SSO), biometric authentication (most often face or fingerprint recognition), Federated Identity Management (FIM), and Fast Identity Online (FIDO). All of these mechanisms aim to increase security but also be usable for users.

It is known that many users behave insecurely from time to time and may have their online accounts compromised. Having an inaccurate or insufficient *mental model* of how online authentication technologies work may be one of the reasons users behave insecurely or sometimes even too cautiously. For instance, users often believe that using a long password which contains their name and birthday is more secure, but in fact long passwords are not more secure if they contain easily guessable information. On the other hand, people think that Single Sign-on authentication (SSO) will share their password and much other personal information with the service they wish to use, so many do not use this form of authentication (Petrie & Sreekumar, 2024; Petrie, Sreekumar, & Shahandashti, 2024). In fact, some information is shared, but never the user's password. Thus, users' inaccurate mental models may lead them to act too

[1] Also at Taif University, Taif, Saudi Arabia. emotaibi@tu.edu.sa

cautiously, not taking advantage of a convenient and possibly more secure authentication method.

Of course, one does not need to have a completely *accurate* mental model to be able to use a digital technology effectively. Most of us do not understand how our computers and smartphones work, yet we use them, mostly effectively every day. However, in the case of authentication technologies, particular inaccuracies in people's mental models can lead to either insecure use or poor user experience. For this reason, we prefer to conceptualise mental models of authentication technologies as *sufficient* or *insufficient,* depending on whether they support users in acting securely in relation to their online accounts or not.

The ultimate objective of this programme of research is to understand more about users' mental models of different authentication technologies and to investigate whether common insufficient models lead to particular security problems (either acting insecurely or too cautiously). This will result in recommendations for authentication technology designers about how to improve the designs of these technologies and make appropriate information available to users to enable them to build sufficient mental models of the technologies. In addition, it will help in the provision of educational materials to guide users in developing more sufficient mental models of authentication technologies so they can act more securely and have better user experiences.

As a first study in this programme of research, an online survey was conducted on the use of and concerns about a range of authentication technologies by a sample of British university staff and students. Although this study did not directly investigate participants' mental models of the technologies, the survey will provide useful information in itself about which authentication technologies participants use most and their concerns about them (which may relate to their mental models of the technologies). It will enable us to choose a set of commonly used authentication technologies to use in further studies which will directly investigate users' mental models of them. As future studies will need to be conducted face-to-face and the only populations available to us with sufficient numbers of participants to work with face-to-face are university staff and students, it made sense to investigate the use of a range of authentication technologies with a sample from these populations, although they are quite specific populations, to have the most accurate information about which authentication technologies to investigate in the future work. Hence, in this work, we aim to answer the following research questions:

RQ1: Which authentication technologies do students and staff use most frequently and how do the frequencies of use differ between the two groups?

RQ2: How do students and staff perceive different authentication technologies in terms of security, usability, trust, understanding and concerns?

RQ3: How do the perceptions of authentication technologies differ between students and staff?

This paper presents the initial analysis of the quantitative data from the survey, further analysis of the qualitative data is taking place, which will provide more information about the concerns of users in such populations about the considered authentication technologies.

2. RELATED WORK

There is an extensive literature on the use of passwords, particularly on the insecure use of passwords, dating as far back as 1979 (Morris & Thompson, 1979). Users frequently make weak passwords, re-use them, write them down, fail to change them often and share them with others, all insecure behaviours (Stobert & Biddle, 2018), although advice on several of these behaviours, e.g. changing passwords often, has changed recently (Poireault, 2024). Taneski, Heričko & Brumen (2014) noted that 35 years after Morris & Thompson's influential paper, the situation had not improved greatly, with much evidence that users were still often creating weak passwords. Mayer & Volkamer (2018) argue that creating weak passwords is often due to users' misconceptions about what makes a strong password and document research identifying 23 common misconceptions, including that the inclusion of numbers, symbols and uppercase letters make passwords automatically stronger, or that letter to symbol substitution (e.g. s to $) will do so. More recently, NordPass (2025) published data from 44 countries, which again found extensive use of weak passwords.

There is less research on the use and concerns about other authentication technologies, partly because they are more recent innovations.

On 2FA authentication, Krol et al. (2015) found that users encountered many usability problems with this technology, and had particular difficulty with dedicated hardware code generators, even changing providers to avoid them. Colnago et al. (2018), studying a university sample in the USA, found that users found it "annoying" but fairly easy to use. Reese et al. (2019) found that users had problems with the system timing out on them and not always having their second device with them. System Usability Scale (SUS) scores were significantly lower for 2FA authentication compared to passwords. Marky et al. (2022) also found that users reported a range of problems and concerns about 2FA including not receiving the code on the second device, dedicated second devices failing and the second device not being available.

On fingerprint and face recognition authentication, very few studies could be found about the actual usability of these mechanisms, although there is considerable research about people's attitudes to their use in the larger societal context, particularly face recognition software (e.g. Zhang et al., 2021). Before the widespread use of these systems in personal devices, detailed studies of the usability of different devices were made (Furman et al., 2017; Stanton et al., 2016; Theofanos et al., 2007, 2008), but these do not tell us about the problems users have with them in everyday use.

Research on SSO/FIM has found that users have security concerns and inaccurate mental models about how these technologies work. Bauer et al. (2013) investigated Google, Facebook, and Google+ FIM provisions and found that participants' perceptions of the information being shared between the identity provider and the target service were largely influenced by their preconceptions. Participants also emphasised the importance of being informed about the information being shared. More recent studies confirmed that users still avoid using SSO/FIM and express doubt about their security. Balash et al. (2022) reported that although more than half of their participants used SSO, most of them were worried about the process exposing personal information, such as their email addresses. Petrie & Sreekumar (2024) found that over 75% of their participants use SSO either regularly or occasionally, on different online services, finding it easy and quick. However, both users and non-users raised security concerns, had misconceptions about how it works, and overestimated the information shared from their accounts, leading them to avoid using SSO for services where it would be safe.

A small number of studies have investigated and compared users' attitudes and concerns about multiple authentication technologies. Notably, Zimmerman & Gerber (2017) conducted a laboratory study of 8 methods: text and graphical password, gesture, fingerprint, face, iris, speech and ear shape recognition. Participants only undertook one authentication with each system and then rated it on a number of dimensions. The most preferred technology was fingerprint recognition and the least preferred was gesture recognition. There were no significant differences in the ratings of perceived security or effort of using the different technologies, but there were significant differences in the level of concerns about privacy, with fingerprint recognition having the highest level of concern and gesture recognition having the lowest level, surprisingly reversing the results for preferences.

Although there have been a small number of comparative studies considering multiple authentication technologies, no recent study has investigated the prevalence of use and concerns about such technologies that are used on an everyday basis. Given the everchanging landscape of such ecosystems, this survey aims to provide an up-to-date and comparative overall view of the authentication technologies most frequently used by UK university student and staff and their concerns, perceptions of security, trust and usability and their understanding of and confidence in using such technologies, as well as providing a basis for our further research.

3. METHOD

3.1 Participants

Participants were recruited from the UK population of university staff (in all roles, including academic and administrative staff) and students. The sample recruited included 70 students and 59 staff members, making 129 participants in total. The demographics of the participants are summarized in Table 1.

The sample of students was reasonably balanced between men and women, but the staff sample had a low proportion of men. However, this difference was not statistically significant (chi-square = 1.24, df = 1, n.s.). The age range for both the staff and student samples was large, but not surprisingly, the median age for the staff members was more than a decade older than that for the students.

46 (65.7%) of the students were studying for a Bachelor's degree, 17 (24.3%) for a Master's and 7 (10.0%) were undertaking research degrees. They were studying a very wide range of subjects, fairly evenly distributed between areas such as Business and Economics, Law, Computer Science, Social Sciences, Humanities, Physical Sciences and Health/Medical Sciences. Only two students said they were studying cybersecurity.

16 (27.1%) of the staff were teaching or research staff, with the remaining 43 (72.9%) being administrative and professional staff. They worked in a very wide range of departments including both sciences and humanities, as well as administrative departments of institutions.

28 (40.0%) of the students reported that they had received some training in online security compared with 55 (93.2%) of the staff. This meant that significantly fewer students than staff had received this kind of training (chi-square = 39.52, $p < 0.001$).

Participants rated their expertise on three areas: computing, the web/internet and online security using 7-point rating items (from "not at all expert": 1 to "very expert": 7). Both students and staff on average rated their computing expertise significantly above the midpoint of the scale, i.e. that they had good expertise, but there was no significant difference between the ratings of the staff and student samples (Mann Whitney U = −0.025, n.s.).

Both staff and student samples also rated themselves significantly above average on web/internet expertise, again with no significant difference between the two samples (U = 0.11, n.s.). However, the ratings of online security expertise were significantly lower than the midpoint of the scale for the student sample, and not significantly different from the midpoint of the scale for the staff sample. So the student sample on average rated their online security expertise as fairly low, whereas the staff sample rated it as medium. Again, there was no significant difference between the samples (U = 0.20, n.s.).

Given the similarities and differences between the two samples, results are presented for the two samples together, although all analyses were also conducted on each sample separately, and any significant differences will be noted.

Table 1: *Demographics of the participants, number (percentage)*

Sample	Students	Staff	All
N	70	59	129
Gender			
Men:	33 (47.1%)	20 (33.9%)	53 (41.1%)
Women:	36 (51.4%)	33 (55.9%)	69 (53.5%)
Non-binary/Prefer to self-identify/not to say:	1 (1.4%)	6 (10.2%)	7 (5.4%)
Age			
Median	25.5	37.5	31.0
Range	18 – 57	24 – 73	18 – 73
Training in online security	28 (40.0%)	55 (93.2%)	
Expertise in computing			
Median (SIQR)	5.0 (1.5)	5.0 (1.0)	5.0 (1.5)
Z, p	Z = 2.48, p = .013	Z = 2.60, p = .009	Z = 3.59, p < .001
Expertise in Web/internet			
Median (SIQR)	5.0 (1.0)	5.0 (1.5)	5.0 (1.0)
Z, p	Z = 2.79, p = .005	Z = 2.93, p = .003	Z = 4.05, p < .001
Expertise in online security			
Median (SIQR)	3.0 (1.0)	3.0 (1.0)	3.0 (1.0)
Z, p	Z = 2.43, p = .015	Z = −1.53, n.s.	Z = −2.78, p = .005

3.2 Questionnaire

A questionnaire was developed and deployed using the Qualtrics online surveys (qualtrics.com). It covered the use and concerns about 7 authentication technologies: passwords, passcodes, face and fingerprint recognition (abbreviated to FaceID and Fingerprint respectively), two-factor authentication (2FA), single sign-on (SSO) and fast identity online authentication (FIDO). Explanations of each of these technologies was provided in the questionnaire, to ensure that participants were clear what was being asked about. A mix of multiple choice, rating and open-ended questions was used to make the questionnaire easy to complete but to collect sufficiently detailed quantitative and qualitative data. The full questionnaire is available from the authors.

3.3 Procedure

The questionnaire was publicised using three different channels in April 2025 for a period of two weeks: on the Prolific research participant recruitment platform (prolific.com), on the University of York staff newsletter and on a number of online mailing lists and groups for HCI researchers, including the BCS HCI jiscmail list. Participants who responded on the Prolific platform received a payment of GBP 2.00, as required by that platform. Participants who responded to the other advertisements were offered the opportunity to enter a prize draw for one of 10 Amazon gift vouchers worth GBP 10.00 each.

The median time taken to complete the questionnaire was 10 minutes 43 seconds (semi-interquartile range, SIQR: 241.5 sec). Staff spent significantly longer completing the questionnaire (median: 11 min 59 sec, SIQR: 340.5 sec) compared to students (median: 9 min 15 sec, SIQR: 165.5 sec) ($Z = 3.64$, $p < 0.001$). The study received ethical approval from The University of York's Physical Sciences Ethics Committee.

3.4 Data analysis

The chi-square test was used to compare differences in frequencies of participants reporting As rating items were used and the distributions of responses were often very skewed, non-parametric statistics were used in the analyses. Wilcoxon Signed-Rank Test was used to assess whether ratings differed significantly from the midpoint of the rating scale, Mann-Whitney U Test was used to assess whether the staff and student sample ratings differed from each other. As sample sizes for both

groups were larger than 30, the Z value approximation was used, rather than the T or U value. To compare the ratings between the different technologies, the Related Samples Friedman Test (Q) was used, with post-hoc comparisons to identify which pairs of technologies differed significantly from each other.

To assess effect sizes, for the Wilcoxon and Mann-Whitney Test, the r statistic was used. For the Related Samples Friedman Test, Kendall's W was used.

4. RESULTS

We provide the results in this paper of the quantitative analysis of the data collected. Answers to open-ended questions on specific concerns our participants expressed about the considered technologies are yet to be analysed and hence we leave the results of the qualitative analysis to future publications.

Results on RQ1: Table 2 shows the number of participants using each of the seven authentication technologies and their frequency of use, rated on a 7-point item ("never": 1 to "very frequently": 7). Passwords were used by all participants who rated their use as "very frequently" whereas FIDO was only used by 19 (14.7%) participants, who rated their use as "occasionally". In terms of the frequency of use, ratings of all technologies were significantly above the midpoint of the scale (despite several of them having medians of the midpoint of 4, due to the weighting of the scores) apart from Fingerprint and FIDO which had ratings significantly below the midpoint, so these two technologies are the least used. Some of the effect sizes for the significant differences were large, but some were only moderate. There were three significant differences between the frequencies of use in the two samples, with more staff using passwords, 2FA and SSO than students. Again, some effect sizes were large and some were moderate.

Results on RQ2: Participants rated their agreement with seven statements about each authentication technology they used (see Table 3): whether they think it is secure; whether they trust it; whether it is easy to use; whether they are confident about using it; whether they understand how it works; whether they have concerns about it; and whether they would like to know more about how it works, again on 7-point items ("strongly disagree": 1 to "strongly agree": 7). The ratings were compared with the midpoint of the scale ("neither agree nor disagree"). Effects sizes were generally large or occasionally moderate, apart from on FIDO, for which they were small or minimal and on the rating of wanting to know more about the technology, for which they range across the whole scale, from large to minimal. All the technologies were rated significantly positively for security, trust, participants' confidence in using them and understanding of them. All the technologies were also rated significantly positively in term of ease of use, apart from FIDO which was rated as neutral in terms of ease of use (FIDO had the smallest number of users in the sample, which may be affecting this result). In terms of concerns about the technologies, all the technologies were rated significantly negatively, meaning that participants had low levels of concerns about them.

We believe a more complex picture may emerge when we analyse the follow-up open-ended question asking participants to elaborate on any concerns. Although this question was optional, many participants provided answers. For example, on the question about passwords, 112 (86.8%) of participants mentioned concerns and on the SSO question 39 (43.8% of those using SSO) mentioned concerns.

In terms of whether participants are interested to know more about how the technologies work (a question of interest in relation to our work on users' mental models of the technologies), all the technologies were rated significantly negatively, meaning participants were not particularly interested in knowing how they work, apart from FIDO, which was rated neutrally.

An analysis was undertaken to compare the ratings of the different authentication technologies on the seven aspects (see Table 4). This showed that there were significant differences between the technologies on four of the seven aspects (although the overall comparison was only significant on two aspects, with seven technologies, it was not surprising that individual post-hoc comparisons between technologies were significant). These were security, trust, ease of use and concerns. On security, SSO was perceived as significantly less secure than a number of the other authentication technologies (2FA FaceID, Fingerprint or FIDO). It was also less trusted than FaceID or FIDO. FaceID was considered significantly easier to use than 2FA or FIDO. Finally, there were significantly lower levels of concerns about FIDO than Password, Passcode, Fingerprint, SSO and 2FA.

Results on RQ3: Another analysis was undertaken to compare staff and students' ratings (see Table 5). This showed differences on their perceptions of 2FA and Fingerprint authentication. Students perceived 2FA as more secure than staff and corresponding had lower levels of concern about it. Similarly, on Fingerprint, students perceived it as more secure, they trusted it more and had more confident in using it than staff. They also had less concerns about it than staff. In all cases, the effect sizes were small.

Table 2: *Use of the different authentication technologies*

Authentication Technology	Students N (%) Frequency: Median, SIQR Differ from midpoint?	Staff N (%) Frequency: Median, SIQR Differ from midpoint?	All N (%) Frequency: Median, SIQR Differ from midpoint? Difference staff-students
Password	70 (100.0%) 7.0 (0.5) Z = 7.31, p < 0.001 r = 0.85 (large effect)	59 (100.0%) 7.0 (0.0) Z = 7.25, p < 0.001 r = 0.85 (large effect)	129 (100.0%) 7.0 (0.5) Z = 10.26, p < 0.001 r = 0.84 (large effect) U = 2.85, p = 0.004 r = 0.23 (small effect)
2FA	65 (92.9%) 4.0 (1.0) Z = 2.62, p = 0.009 r = 0.30 (moderate effect)	59 (100.0%) 6.0 (1.0) Z = 6.03, p <0.001 r = 0.70 (large effect)	124 (96.1%) 5.0 (1.5) Z = 7.37, p < 0.001 r = 0.60 (large effect) U = 4.53, p < 0.001 r = 0.36 (moderate effect)
Passcode	61 (87.1%) 4.0 (2.0) Z = 1.13, n.s. r = 0.13 (small effect)	53 (89.8%) 4.0 (1.5) Z = 1.53, n.s. r = 0.18 (small effect)	114 (88.4%) 4.0 (2.0) Z = 4.47, p < 0.001 r = 0.36 (moderate effect) U = −1.62, n.s. r = 0.13 (small effect)
SSO	38 (54.3%) 2.0 (1.5) Z = −4.19, p < 0.001 r = 0.48 (moderate effect)	51 (86.4%) 4.0 (2.0) Z = 0.84, n.s. r = 0.09 (minimal effect)	89 (69.0%) 4.0 (1.0) Z = 3.44, p < 0.001 r = 0.28 (small effect) U = 3.59, p < 0.001 r = 0.29 (small effect)
FaceID	43 (61.4%) 4.0 (3.0) Z = −0.76, n.s. r = 0.09 (minimal effect)	29 (49.2%) 1.0 (2.5) Z = −2.78, p = 0.005 r = 0.32 (moderate effect)	72 (55.8%) 4.0 (2.5) Z = 6.10, p < 0.001 r = 0.49 (moderate effect) U = −1.62, n.s. r = 0.13 (small effect)
Fingerprint	37 (52.9%) 2.0 (1.5) Z = −3.97, p < 0.001 r = 0.46 (moderate effect)	24 (40.7%) 1.0 (1.5) Z = −4.62, p < 0.001 r = 0.53 (large effect)	61 (47.3%) 1.0 (1.5) Z = 2.92, p = 0.004 r = 0.23 (small effect) U = −1.05, n.s. r = 0.09 (minimal effect)
FIDO	9 (12.9%) 1.0 (0.0) Z = −7.90, p < 0.001 r = 0.91 (large effect)	10 (16.9%) 1.0 (0.0) Z = −7.09, p < 0.001 r = 0.82 (large effect)	19 (14.7%) 1.0 (0.0) Z = −3.12, p = 0.002 r = 0.25 (small effect) U = 0.72, n.s. r = 0.06 (minimal effect)

Table 3: *Ratings for each of the authentication technologies on the seven aspects (Medians, SIQRs and effect size – exact values of effect size omitted to economize on space)*

	Password	**2FA**	**Passcode**	**SSO**	**FaceID**	**Fingerprint**	**FIDO**
Secure	5.0 (1.0) *** Large	6.0 (0.5) * Large	5.0 (1.0) *** Large	5.0 (1.0) *** Large	7.0 (0.5) *** Large	6.0 (0.5) *** Large	6.0 (0.0) *** Small
Trust	6.0 (0.5) *** Large	6.0 (0.5) *** Large	5.0 (1.0) *** Large	5.0 (1.0) *** Large	6.5 (1.0) *** Large	6.0 (0.5) *** Large	6.0 (0.5) *** Small
Easy	6.0 (0.5) *** Large	5.0 (1.5) *** Small	6.0 (1.0) *** Large	6.0 (1.0) *** Large	7.0 (0.5) *** Large	7.0 (0.5) *** Large	4.0 (1.5) n.s. Minimal
Confident	6.0 (1.0) *** Large	6.0 (1.0) *** Large	6.0 (1.0) *** Large	6.0 (1.0) *** Large	7.0 (0.5) *** Large	6.0 (0.5) *** Large	5.0 (0.5) ** Small
Understand	6.0 (1.0) *** Large	6.0 (1.0) *** Large	6.0 (1.0) *** Large	6.0 (1.0) *** Large	6.5 (1.0) *** Large	6.0 (0.5) *** Large	5.0 (1.0) * Small
Concerns	4.0 (1.0) N*** Moderate	1.0 (1.0) N*** Large	4.0 (1.0) N*** Moderate	2.0 (1.5) N*** Moderate	2.0 (1.5) N*** Large	2.0 (1.0) N*** Large	1.0 (0.5) N*** Small
Know more	4.0 (1.0) N*** Small	2.0 (1.0) N*** Large	2.5 (1.5) N*** Moderate	3.0 (1.5) N*** Large	3.0 (2.0) N*** Small	4.0 (1.5) N** Small	4.0 (1.5) n.s. Minimal

n.s.: not significant; * indicates p < 0.05; ** indicates p < 0.01; *** indicates p < 0.001; N: negative relationship

Table 4: *Comparison between the authentication technologies on the seven aspects (FIDO omitted due to small number of participants using that technology) (N = 23)*

	Omnibus comparison	**Pairs of technologies which differ significantly**
Secure	Q = 34.86, p < 0.001 W = 0.31 (moderate effect)	2FA perceived as significantly more secure than SSO, Passcode, and Password (p < 0.05)
Trust	Q = 21.50, n.s. W = 0.19 (small effect)	SSO significantly less trusted than 2FA and FaceID (p < 0.05)
Easy	Q = 29.63, p < 0.001 W = 0.26 (small effect)	FaceID significantly easier to use than 2FA or Fingerprint (p < 0.01)
Confident	Q = 6.93, n.s. W = 0.06 (minimal effect)	No significant differences
Understand	Q = 3.87, n.s. W = 0.03 (minimal effect)	No significant differences
Concerns	Q = 38.17, p < 0.001 W = 0.33 (moderate effect)	Significantly higher concerns about Passcode than Fingerprint (p < 0.05) Significantly higher concerns about Passwords than SSO, 2FA and Fingerprint (p < 0.05)
Know more	Q = 9.99, n.s. W = 0.08 (minimal effect)	No significant differences

5. DISCUSSION AND CONCLUSIONS

This study investigated the use of and concerns about a range of modern authentication technologies among British university staff and students. Preliminary results show varying levels of use of the different technologies, with all participants using passwords, in spite of their demise having been predicted for many years, e.g. by Bill Gates in 2004 (Furnell, 2005). But this result is in line with other recent research which has found that people still use passwords very frequently (Stobert & Biddle, 2018; Woods & Siponen, 2025). On the other hand, FIDO is yet to be frequently used, despite being promoted as a more secure authentication mechanism, and a replacement for passwords (Angelogianni et al., 2024; Ulqinaku et al., 2021).

The study found that there were significant differences between staff and students in the frequency of use of three authentication technologies: passwords, 2FA and SSO. These differences may reflect both the personal and work lives of these two groups. 2FA and SSO are both widely used in institutional contexts including universities, to provide strong security for sensitive information, so it is very likely that many university staff use them extensively in their work, which may not be so relevant to the student group, although they should be securing their personal educational materials. It was interesting that nearly all the staff participants reported having to received training in online security (93.2%) compared to less than half of the student participants (40.0%), so they may be much more aware of the importance of using strong security for their work materials and it may be a requirement of their institution. It is also possible that being an older group, the staff have accumulated more online accounts for both work and personal use, many of which still require

***Table 5:** Comparison of the authentication technologies by staff and students*

Authentication Technology	Significant differences
Password	None
2FA	Students perceive 2FA as more secure than staff Student median: 7.0 (0.5) vs Staff median: 6.0 (0.5) Z = −2.48, p = 0.013 r = 0.20 (small effect) Staff more concerned about 2FA than students Staff median: 2.0 (1.0) vs Student median: 1.0 (0.5) Z = 2.18, p = 0.033 R = 0.18 (small effect)
Passcode	None
SSO	None
FaceID	None
Fingerprint	Students more confident in using Fingerprint than staff Student median: 7.0 (0.5) vs Staff median: 6.0 (1.0) Z = −2.19, p = 0.029 r = 0.20 (small effect) Students perceive Fingerprint as more secure than staff Student median: 7.0 (0.5) vs Staff median: 6.0 (2.5) Z = −2.57, p = 0.010 r = 0.21 (small effect) Students trust Fingerprint more than staff Student median: 7.0 (0.5) vs Staff median: 6.0 (1.0) Z = −2.80, p = 0.005 r = 0.23 (small effect) Staff more concerned about Fingerprint than students Staff median: 2.0 (1.5) vs Student median: 1.0 (0.5) Z = 2.30, p = 0.022 r = 0.19 (small effect)
FIDO	None

passwords, so they use passwords more frequently than the younger group of students. The survey asked participants about what kinds of accounts they use the different authentication technologies for, but these questions have not yet been analysed. They may well help understand these different patterns of use of the authentication technologies in greater depth.

The considered authentication technologies were largely perceived as secure, trustworthy and easy to use, participants were confident in using them and had low levels of concerns about them. These are interesting results in light of previous literature which has found that participants have a range of usability problems with authentication, often have concerns, particularly about security. However, as mentioned, the ratings may not be telling the whole story here, and the analysis of the open-ended questions on participants' concerns about the technologies may show a less positive picture.

There were interesting differences between the attitudes about the different authentication technologies, with SSO/FIM perceived as less secure and less trusted than a number of the other technologies, and participants had more concerned about this technology. This finding is in line with previous research about SSO/FIM, particularly recent research in the UK which found that both users and non-users of SSO/FIM perceive it as insecure and they have numerous concerns and misconceptions about it (Petrie & Sreekumar, 2024; Petrie, Sreekumar & Shahandashti, 2024).

In addition, there were interesting differences between the two samples of participants, with students generally being more positive about 2FA and Fingerprint authentication and having lower levels of concern. Given that the staff participants were much more likely to have had some training in online security issues than the students, this is not surprising, as they may well have been more aware of the risks with online systems. It would be interesting to compare university staff with a similar age group of adults to investigate whether the difference is due to this training or to other factors. The analysis of the open-ended questions on concerns may also explain these differences further. The more positive attitudes of the younger, student group are in line with other research about age differences in attitudes to online authentication and security. Merdenyan & Petrie (2025) compared samples of younger and older people in the UK (albeit the older people were much older than the current sample, 65 years and older) and found that the younger sample were much less concerned about online authentication practices, made weaker passwords and used less strategies for making and remembering their passwords than the older sample. Similarly, in the USA, Yuan et al. (2024) found younger people were more likely to share their passwords than older users, an insecure practice.

The study focused on university staff and students, which provides valuable insights into the use and concerns of authentication technologies within an academic environment. Future work could broaden the scope by including a wider range of demographic groups, particularly non-academic participants. That would allow for a richer understanding of how different populations engage with and manage security in their everyday lives, highlighting variations in usage, perceptions, and concerns that may not emerge in a university context.

Overall, this study has provided a useful snapshot of the use of authentication technologies by two groups in the UK, university staff and students, and their

concerns about these technologies. Interesting differences were found in the use and attitudes to the different technologies and the concerns participants have about them. In addition, there were interesting differences between the staff and student groups, which may reflect differences in their age and experience, but also differences in their current context of the use of online systems, the former using them very extensively for work as well as in their personal lives, the latter for their education and personal lives.

Further analyses of the survey results, the answers to questions about the types of services participants use the different authentication technologies for, and the open-ended questions on their specific concerns about the technologies, should provide more detailed information on these issues. Furthermore, the results provide us with clear guidance as to the authentication technologies we will now study in more detail, to investigate the effects of users' mental models of how they work on their attitudes and behaviour.

We hope that findings from the qualitative analysis of open-ended questions provide us with a richer understanding of misconceptions and concerns regarding the use of the considered authentication technologies. This would enable the development of educational materials aimed at addressing the misconceptions identified and helping users develop mental models that are better aligned with the design principles of such technologies, ultimately leading to better decision making and improved security behaviour.

ACKNOWLEDGEMENTS

We would like to thank all the participants in this study for their time and effort in contributing to the research. We would also like to acknowledge the support of the Deanship of Graduate Studies and Scientific Research, Taif University, Kingdom of Saudi Arabia for funding Ibtihail Alotaibi's work on this project.

6. REFERENCES

Angelogianni, A., Politis, I., & Xenakis, C. (2024). How many FIDO protocols are needed? Analysing the technology, security and compliance. *ACM Computing Surveys*, *56*(8), 1–51.

Balash, D.G., Wu, X., Grant, M., Reyes, I., & Aviv, A.J. (2022). Security and privacy perceptions of third-party application access for Google accounts. Proceedings of the 31st USENIX Security Symposium.

Bauer, L., Bravo-Lillo, C., Fragkaki, E., & Melicher, W. (2013). A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality. Proceedings of the 2013 ACM Workshop on Digital Identity Management. ACM Press.

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). "It's not actually that horrible" Exploring Adoption of Two-Factor Authentication at a University. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1–11). https://doi.org/10.1145/3173574.3174030

Egelman, S. (2013). My profile is my password, verify me! the privacy/convenience tradeoff of Facebook connect. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris, France. (2013).

Furman, S. M., Stanton, B. C., Theofanos, M. F., Libert, J. M., & Grantham, J. D. (2017). Contactless fingerprint devices usability test. US Department of Commerce, National Institute of Standards and Technology.

Furnell, S. (2005). Authenticating ourselves: will we ever escape the password? Network Security, 3, 8–13

Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. NDSS Workshop on Usable Security (USEC 2015).

Marky, K., Ragozin, K., Chernyshov, G., Matviienko, A., Schmitz, M., Mühlhäuser, M., ... & Kunze, K. (2022). "Nah, it's just annoying!" A deep dive into user perceptions of two-factor authentication. ACM Transactions on Computer-Human Interaction, 29(5), 1–32. https://doi.org/10.1145/35035

Mayer, P., & Volkamer, M. (2018). Addressing misconceptions about password security effectively. In Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust, pp. 1–-27. ACM Press, New York. https://doi.org/10.1145/3167996.3167998

Merdenyan, B., & Petrie, H. (2025). Password Authentication for Older People: Problems, Behaviours and Strategies. In Law, E., Perez, M.L. & Mulvenna, M. (Eds.), Proceedings of 11th International Conference on Information and Communication Technology for Ageing Well and e-Health (ICT4AWE 2025). https://www.scitepress.org/Link.aspx?doi=10.5220/0013299800003938

Morris, R. and Thompson, K. (1979). Password Security: A Case History. Communications of the ACM, 22(11), 594–597. https://doi.org/10.1145/359168.359172

NordPass (2025). Most common passwords. https://nordpass.com/most-common-passwords-list/

Petrie, H. & Sreekumar, G. (2024). Passwords and single sign-on: Use, security, and understanding for online accounts. In Proceedings of the 37th International BCS Human-Computer Interaction Conference (BCS HCI '24). BCS: London. https://10.14236/ewic/BCSHCI2024.16

Petrie, H., Sreekumar, G. & Shahandashti, S. F. (2024) Understanding users' mental models of Federated Identity Management (FIM): use of a new tangible elicitation method. In Clarke, N., & Furnell, S. (eds) Human Aspects of Information Security and Assurance. HAISA 2024. IFIP Advances in Information and Communication Technology, vol 721. Springer, Cham. https://doi.org/10.1007/978-3-031-72559-3_21

Poireault, K. (2024). NIST scraps passwords complexity and mandatory changes in new guidelines. Infosecurity Magazine, https://www.infosecurity-magazine.com/news/nist-scraps-passwords-mandatory/

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five two-factor authentication methods. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 357–370). https://www.usenix.org/conference/soups2019/presentation/reese

Stanton, B. C., Theofanos, M. F., Furman, S. M., Grother, P. J., Grother, P., & Pritzker, P. (2016). Usability testing of a contactless fingerprint device: Part 2. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.

Stobert, E., & Biddle, R. (2018). The password life cycle. ACM Transactions on Privacy and Security (TOPS), 21(3), 1–32. https://doi.org/10.1145/3183341

Taneski, V., Heričko, M. & Brumen, B. (2014). Password security - No change in 35 years? 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1360–1365 doi: 10.1109/MIPRO.2014.6859779.

Theofanos, M.F., Stanton, B. C., Orandi, S., Micheals, R.J., & Zhang, N.F. (2007). Usability Testing of Ten-Print Fingerprint Capture. Tech. Rep, National Institute of Standards and Technology.

Theofanos, M., Stanton, B., Sheppard, C., Micheals, R., Zhang, N., Wydler, J., ... & Rubin, W. (2008). Usability testing of height and angles of ten-print fingerprint capture. National Institute of Standards and Technology (NIST), Tech. Rep.

Ulqinaku, E., Assal, H., Abdou, A., Chiasson, S., & Capkun, S. (2021). Is real-time phishing eliminated with FIDO? social engineering downgrade attacks against FIDO protocols. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 3811–3828).

Woods, N., & Siponen, M. T. (2025). Questioning a security assumption: are unique passwords harder to remember than reused or modified passwords? *Computers & Security*, 104545.

Yuan, L., Chen, Y, Tang, J., & Cranor, L.F. (2024). Account password sharing in ordinary situations and emergencies: a comparison between young and older adults. In Proceedings on Usable Privacy and Security (SOUPS). USENIX.

Zhang, S., Feng, Y., & Sadeh, N. (2021). Facial recognition: Understanding privacy concerns and attitudes across increasingly diverse deployment scenarios. In Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021) (pp. 243–262).

Zimmermann, V., & Gerber, N. (2017). "If it wasn't secure, they would not use it in the movies"–security perceptions and user acceptance of authentication technologies. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 265–283). Springer International Publishing.