



Deposited via The University of York.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/241936/>

Version: Accepted Version

Proceedings Paper:

ALOTAIBI, IBTIHAL, Petrie, Helen and Shahandashti, Siamak F. (2026) A Comparative Study of British Users' Perception, Use, and Concerns about a Range of Authentication Systems. In: Human Aspects of Information Security and Assurance:20th IFIP WG 11.12 International Symposium, HAISA 2026, Orebro, Sweden, July 6–8, 2026, Proceedings. 20th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2026), 06-08 Jul 2026 IFIP Advances in Information and Communication Technology. Springer Cham, SWE.

Reuse

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:

<https://creativecommons.org/licenses/>

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

A comparative study of British users' perception, use, and concerns about a range of authentication systems

Ibtihal Alotaibi^[0009-0008-5939-4290] Helen Petrie^[0000-0002-0100-9846]

and Siamak F. Shahandashti^[0000-0002-5284-6847]

¹ Department of Computer Science, University of York, York YO10 5DD, UK

{ia893|helen.petrie|siamak.shahandashti}@york.ac.uk

Abstract. Many authentication systems are now available to secure online information. These also need to be usable and trusted by users. There is a considerable body of research on users' perceptions, use, and concerns about individual authentication systems, but little research comparing users' attitudes across a range of current authentication systems. An online survey was conducted investigating these issues with a sample of 129 well-educated British participants. Seven authentication systems were investigated: password, passcode, two factor (2FA), Federated Identity Management (FIM), face and fingerprint recognition, and Fast Identity Online Authentication (FIDO). All, apart from FIDO, were rated as very secure, trustworthy, and easy to use. Participants were confident about using them and generally rated their level of concern about them as low. However, when asked to express any concerns, participants raised a wide range of concerns, which need to be addressed by developers and deployers of these systems.

Keywords: Authentication, Password Authentication, Passcode Authentication, Federated Identity Management, Single Sign-On Authentication, Two-Factor Authentication, Biometric Authentication, Fast Identity Online Authentication.

1 Introduction

There are now numerous authentication methods for users to deal with, from biometric methods such as face and fingerprint recognition to Federated Identity Management (FIM, often confused with Single Sign-On by users) and various forms of two-factor (2FA) and multi-factor (MFA) authentication. All these methods have different advantages and disadvantages for security and for users. From the users' perspective, there is a growing body of research on their perceptions, use, and concerns about individual methods, but little research has investigated these issues across a range of different methods, in order to be able to comparatively assess them. Therefore, this study set out to investigate the use, perceptions, and concerns of seven different authentication methods with a well-educated sample of British users: password, passcode, FIM, 2FA, face recognition (FaceID), fingerprint recognition (FingerID) and Fast Identity Online Authentication (FIDO).

2 Related Work

There is an extensive body of research on the use and misuse of passwords as well as users' concerns about both password systems and their own use of them, and more recently password managers [34] which is beyond the scope of this paper to review. It is well-established that users frequently make weak passwords, re-use them, write them down, fail to change them often and share them with others, all insecure behaviours. Studies have found a range of perceptions of passwords and their security. For example, Mayer & Volkamer [23] in an extensive literature review found that users had many misconceptions about password security. On the other hand, Shay et al. [31] found that although people found strong password policies annoying, they appreciated that they made their online information more secure.

There is also a small body of research on passcodes, largely on their use in automated banking machines, which is now becoming less common. Studies found that across a number of countries (Germany, Sweden and the UK) the majority of users do not shield their passcode when entering it, which may be insecure and that users worry about forgetting their passcodes, although typically they are short [13, 25, 35].

Research on the use and concerns about 2FA authentication has found that users have usability and reliability problems with these systems, for example the lack of availability of a required second device and time out issues [20, 22, 28]. However, Reynolds et al. [29] analyzed a data corpus of 2FA log data and estimated that users only spent approximately 15 minutes in a year on 2FA authentication, although more than one in 20 authentication attempts did not end successfully. Other studies found that 2FA is annoying but easy to use [11] or that it makes users feel more secure [14]. There is also some research specifically on FIDO, which overlaps with research on 2FA. Ciolino et al [10] found, as had a number of previous studies, that users have concerns about the benefits of security keys in FIDO and their security purpose.

Research on FIM is extensive. Petrie et al. [27] provided a recent review of research on this topic. A number of studies have found that users are reluctant to use FIM, often due to misconceptions about how it works and in particular how secure it is [2, 8, 15, 26, 27, 32]. On the other hand, Ruoti et al. [28] found that users preferred FIM to other authentication processes, but they also wanted to augment it with site-specific passwords.

On biometric authentication, such as face or fingerprint recognition methods, there has been considerable research on attitudes to the technologies in general [e.g. 9, 16] but less on use and concerns. Before the widespread use of these systems in personal devices, detailed studies of the usability of different devices were made [e.g. 33], but these do not tell us about concerns users have with them in everyday use. Bhagavatula et al. [5] in a lab study found face and fingerprint authentication easy to use, although there were practical limitations such as light level and sticky or wet fingers affecting fingerprint authentication. However, in their survey of use in everyday life, many respondents reported ceasing the use of face authentication, often due to reliability issues. DeLuca et al. [12] also found that many respondents had ceased using face authentication, but far fewer had ceased fingerprint authentication. Reasons included reliability and usability issues. Baqeel and Saeed [4] found that users were selective about when

they used face authentication, being less likely to use it in financial situations, suggesting less trust in this method. They also found practical usability limitations such as the system failing when users wore glasses or head coverings. Lassak et al. [21] found that 67% of survey respondents thought their biometric information was sent to the website on authentication, creating security concerns.

Few studies could be found which assess users' perceptions, use and concerns across different authentication systems. Several papers have proposed frameworks for evaluating authentication processes which include usability [7, 24], but do not validate these frameworks with users. An early study [18] conducted a large survey with university students in the USA and found considerable uncertainty and misconceptions about authentication systems. The survey asked about password, biometric and token-based authentication. Passwords were rated highly and participants were interested in biometric authentication, although only half the sample had used this form of authentication. There were also interesting differences in the perceived usefulness of authentication systems in different contexts, such as financial transactions versus general computer access. Ruoti et al [30] compared FIM, email-based and QR-based authentication in two simulated applications, an online forum and an online banking site. Participants completed authentication tasks with these applications and answered questions about them. Participants preferred FIM, but they wished to augment it with site-specific low-entropy passwords. They were also interested in biometric authentication. Finally, Zimmermann & Gerber [36] simulated eight different authentication systems: text and graphical passwords and a range of biometric systems (gesture, fingerprint, face, iris, speech and ear shape). Text passwords were the most preferred, due to habit, simplicity and perceived security. Of the biometric systems, fingerprint and iris systems were the most preferred, being seen as secure, although these systems also presented concerns about privacy.

3 Research Method

3.1 Participants

Participants were recruited from students and staff (in all roles, including academic and administrative) at higher education institutions (HEIs) in the UK. A total of 129 participants were recruited, 70 students and 59 staff. The demographics of the participants are summarized in Table 1. The sample was slightly skewed toward women participants, as is often the case in voluntary exercises. The age range was wide, although over 40% of the sample were under 30. A majority of the students were studying at undergraduate level (46, 65.7%), with the remainder studying at graduate level, on both taught and research programs. The majority of the staff were in administrative and technical roles (43, 72.9%) with the remainder in teaching roles. Both students and staff were from a wide range of disciplines. Over half the participants reported having received some training in online security. However, significantly more staff had received this kind of training (40.0% of the students versus 93.2% of staff, chi-square = 39.52, $p < 0.001$). This may be because training in this area is compulsory for staff in many UK HEIs.

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

Gender	
Men:	53 (41.1%)
Women:	69 (53.5%)
Non-binary/Prefer to self-identify/not to say	7 (5.4%)
Age	
Median	31.0
Range	18 – 73
Training in online security	83 (64.3%)
Expertise in computing	
Median (SIQR)	5.0 (1.5)
Different from midpoint	$Z = 3.59, p < .001$
Expertise in Web/internet	
Median (SIQR)	5.0 (1.0)
Different from midpoint	$Z = 4.05, p < .001$
Expertise in online security	
Median (SIQR)	3.0 (1.0)
Different from midpoint	$Z = -2.78, p = .005$

Participants rated their expertise on three areas: computing, the web/internet and online security using 7-point rating items (from “not at all expert”: scored as 1 to “very expert” scored as 7). On computing and the web/internet they typically rated themselves as above the midpoint of the scale of expertise, so reasonably expert. But on online security they typically only rated themselves at the midpoint of the scale, so moderately expert.

3.2 Online Questionnaire

A questionnaire was developed and deployed using the Qualtrics online survey software (qualtrics.com). It covered the use and concerns about seven authentication methods: passwords, passcodes, FaceID, FingerID, 2FA, FIM, and FIDO. Explanations of each of these technologies were provided in the questionnaire, to ensure that participants were clear about what was being asked.

For each authentication method, participants first asked if they used it and if so, how often (on a 7-point rating item). If they reported using the method, questions asked what kinds of accounts they used it for, their agreement with 7 statements about their experiences with the method (Table 2), again on 7-point rating items. Finally, an open-ended question asked them to explain any concerns they had with the method.

The questionnaire ended with a section to collect demographic information.

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 multiple choice and rating questions were compulsory, but the open-ended questions were optional. The questionnaire is available from the authors.

Table 2: The seven aspects of participants' experience with the authentication method

Statement	Short name
It is an easy method to use	Ease of use
I am confident about using this method	Confidence
It is a secure method for logging in	Security
I trust this method for logging in	Trustworthy
I understand how this method works	Understanding
I would like to know more about how this method works	More knowledge
I have concerns about [method]	Concerns

3.3 Procedure

The questionnaire was publicized 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. Participants who responded on the Prolific platform received a payment of GBP 2.00 (approx. EUR 2.30). Prolific sets the level of payments to participants based on the current “living wage”¹ in the UK. 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 (approx. EU 11.50) each. The data from the two datasets with different compensations were compared and no differences could be detected, so they were combined.

Participants were assured of the confidentiality of the information they provided, that only the three authors would have access to their actual responses and that all public use of the information (including sharing data with other researchers) would be completely anonymous. Participants were free to withdraw from the study or withdraw their data after the study, but were asked to notify the researchers within a week of completing the questionnaire if they wished to do so (to avoid having to re-analyze the data). No participant withdrew.

The median time taken to complete the questionnaire was 10 minutes 43 seconds (semi-interquartile range, SIQR: 241.5 sec).

The study received ethical approval from the Physical Sciences Ethics Committee at the University of York.

3.4 Data Analysis

As distributions on the rating items were often skewed, non-parametric statistics were used in the analyses. Wilcoxon Signed-Rank Tests were used to assess whether ratings differed significantly from the midpoint of the rating scale. As the sample size was larger than 30, the Z value approximation was used. To compare the ratings between the different technologies, Related Samples Friedman Tests were used, with post-hoc comparisons to identify which pairs of technologies differed significantly from each other.

¹ <https://www.livingwage.org.uk/what-real-living-wage>

4 Results

Table 3 summarizes the number of participants who reported having used the seven authentication systems and their frequency of use (from “never”: 1 to “very frequently”: 7). These ranged from all participants reporting using password authentication very frequently, to less than 15% of participants using FIDO. All ratings of frequency were significantly higher than the midpoint of the scale, apart from FIDO which was significantly lower than the midpoint.

Table 3. Participants’ use of the seven authentication methods

Authentication System	N (%)	Frequency: Median, SIQR	Difference from midpoint
Password	129 (100.0%)	7.0 (0.5)	$Z = 10.26, p < 0.001$
2FA	124 (96.1%)	5.0 (1.5)	$Z = 9.58, p < 0.001$
Passcode	114 (88.4%)	4.0 (2.0)	$Z = 4.47, p < 0.001$
FIM	89 (69.0%)	4.0 (1.0)	$Z = 3.44, p < 0.001$
FaceID	72 (55.8%)	4.0 (2.5)	$Z = 6.10, p < 0.001$
FingerID	61 (47.3%)	4.0 (1.0)	$Z = 2.92, p = 0.004$
FIDO	19 (14.7%)	1.0 (0.0)	$Z = -3.12, p = 0.002$

The number of different authentication systems participants use ranged from 2 to 7, with a median of 5. Thus, participants are using a number of different methods for authentication which may be confusing, as well as adding to their cognitive load of needing to remember different procedures as well as passwords or codes. This issue was not explored in this study but would be of interest for future research.

Table 4 summarizes the ratings of seven different statements about each authentication system. The table also summarizes the tests of whether the ratings differ from the midpoint of the rating scale. All the authentication systems are perceived as positively secure and trustworthy, and participants are positively confident about using them and believe they understand how they work. Perhaps due to the fact that they think they know how they work, participants have relatively low interest in knowing more about how the systems work. Finally, all the methods apart from FIDO are perceived as easy to use, with FIDO having moderate ratings for ease of use.

Table 5 summarizes the comparisons between the seven authentication methods on each statement. There were significant differences in perceptions of security, trust, ease of use, and participants concerns.

Table 4: Ratings for each of the authentication methods on seven different aspects (Medians, SIQRs, test of difference from midpoint, details omitted for clarity of presentation and space)

	Password	2FA	Passcode	SSO	FaceID	FingerID	FIDO
Security	5.0 (1.0) ***	6.0 (0.5) *	5.0 (1.0) ***	5.0 (1.0) ***	7.0 (0.5) ***	6.0 (0.5) ***	6.0 (0.0) ***
Trust	6.0 (0.5) ***	6.0 (0.5) ***	5.0 (1.0) ***	5.0 (1.0) ***	6.5 (1.0) ***	6.0 (0.5) ***	6.0 (0.5) ***
Ease of use	6.0 (0.5) ***	5.0 (1.5) ***	6.0 (1.0) ***	6.0 (1.0) ***	7.0 (0.5) ***	7.0 (0.5) ***	4.0 (1.5) n.s.
Confidence	6.0 (1.0) ***	6.0 (1.0) ***	6.0 (1.0) ***	6.0 (1.0) ***	7.0 (0.5) ***	6.0 (0.5) ***	5.0 (0.5) **
Understanding	6.0 (1.0) ***	6.0 (1.0) ***	6.0 (1.0) ***	6.0 (1.0) ***	6.5 (1.0) ***	6.0 (0.5) ***	5.0 (1.0) *
Concerns	4.0 (1.0) N***	1.0 (1.0) N***	4.0 (1.0) N***	2.0 (1.5) N***	2.0 (1.5) N***	2.0 (1.0) N***	1.0 (0.5) N***
Know more	4.0 (1.0) N***	2.0 (1.0) N***	2.5 (1.5) N***	3.0 (1.5) N***	3.0 (2.0) N***	4.0 (1.5) N**	4.0 (1.5) n.s.

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

Table 5: Comparison between the authentication technologies on the seven aspects (FIDO omitted due to the small number of participants using that technology)

Authentication System	Omnibus comparison	Pairs of technologies which differ significantly
Secure	$Q = 34.86, p < 0.001$	2FA perceived as significantly more secure than SSO, Passcode, and Password ($p < 0.05$)
Trust	$Q = 21.50, n.s.$	SSO significantly less trusted than 2FA and FaceID ($p < 0.05$)
Easy to use	$Q = 29.63, p < 0.001$	FaceID significantly easier to use than 2FA or FingerprintID ($p < 0.01$)
Confident	$Q = 6.93, n.s.$	No significant differences
Understand	$Q = 3.87, n.s.$	No significant differences
Concerns	$Q = 38.17, p < 0.001$	Significantly higher concerns about Passcode than Fingerprint ($p < 0.05$) Significantly higher concerns about Passwords than SSO, 2FA and FingerprintID ($p < 0.05$)
Want to know more	$Q = 9.99, n.s.$	No significant differences

The rating data were complemented by an optional open-ended question about each method participants used, asking them to describe any concerns they have. Both the number of participants answering the question and the type and frequency of concerns

are summarized in Tables 6 to 12. Only concerns mentioned by more than 5% of participants answering about a particular authentication method are listed, although this meant that some of the numbers of participants involved are relatively small for authentication systems for which not many participants answered. Concerns were divided into those related to the authentication system itself and those related to participants' own use of the method.

Passwords used by all participants and were also the method eliciting responses from the most participants (Table 6). This aligns with the fact that they received the highest ratings of concern, along with Passcode authentication (Table 3) and rated significantly higher than SSO, 2FA or FingerID authentication (Table 4). By far the most commonly expressed concern about password authentication was that the system might be hacked or passwords leaked (48.1% of participants answering the question mentioned this concern). Two other concerns about the password system itself were mentioned, whether passwords were encrypted by the system and more general comments that the system was not secure, without specifying why. Participants also mentioned a range of concerns about using passwords which have been extensively documented in previous research.

Table 6: Concerns about password authentication (N using = 129; N replying = 112, 86.8%)

Theme/subtheme	Example quotes	5 (N)
Password system concerns		
Hacks/leaks	Data breaches so other people can get my password (P47)	48.1 (62)
Encryption	How my passwords are stored (encrypted / plain text etc) (P57)	7.0 (9)
General/unspecified security concerns	Passwords without some kind of MFA are not very secure (P129)	14.0 (18)
Password Use concerns		
Remembering	I might forget them (P94)	16.3 (21)
Password re-use	Repetition due to mental saturation meaning I can't remember unique passwords for all accounts (P84)	14.0 (18)
Password strength	I worry my passwords could be easily guessed (P15)	8.5 (11)
Large number of passwords	It can be hard to remember them all if you use different ones for all different accounts (P14)	7.8 (10)
Need to change/reset password	Having to change them frequently as a matter of policy (P81)	5.4 (7)

2FA authentication was the second most used authentication system, by 96.1% of participants. However, less than 40% of participants raised concerns about it. This aligns with the low ratings of concern, although perhaps the number of participants mentioning concerns suggests the rating is optimistically low. On the other hand, perhaps this indicates that these concerns are not particularly severe. As with password authentication, the most frequently mentioned system concern is about it being hacked or data being leaked, although the percentage of participants mentioning this is considerably lower than for password systems (18.4% vs 48.1%). In the case of 2FA,

the concerns about hacking were often that the message could be intercepted. This was also partly reflected in concerns about reliability, participants wondering what has happened if the message does not come through, apart from it meaning the participant cannot log in. Nearly a quarter of participants (22.4%) mentioned general or unspecified concerns, suggesting that they have doubts about the security of the system but are not sure why (which is an interesting contrast to the high ratings of knowing how it works).

Table 7: Concerns about 2FA authentication (N using = 124; N replying = 49, 39.5%)

2FA system concerns		
Hacks/leaks	I feel like the SMS or email can be intercepted and used to hack my account (P64)	18.4 (9)
Reliability	sometimes the code does not come through and I wonder where it has gone (P71)	16.3 (8)
General/unspecified security concerns	the main issue ... is security of the devices receiving the code (P128)	22.4 (11)
2FA Use concerns		
2F Device availability/theft	Reliant on access to phone or email, which may have fallen into the wrong hands (P78)	32.7 (16)
Usability issues	Many 2FA processes are slow and not very "user friendly" (P80)	28.6 (14)

Table 8: Concerns about passcode authentication (N using = 114; N replying = 68, 59.7%)

Passcode system concerns		
Easy to crack/less secure than passwords	passcodes are very small and can easily be brute forced (P40) Don't know if it's as secure as a password (P49)	38.2 (26)
Hacks/leaks	I have the irrational fear I'll be hacked (P23)	20.6 (14)
General/Unspecified/unclear security concerns	not sure how safe and secure they are (P109)	20.6 (14)
Passcode Use concerns		
Remembering	Sometimes digits are difficult to remember, especially when the passcodes themselves are long (P55)	11.8 (8)
Shoulder surfing/smudge attacks	You can find out people passcodes just by looking at where they tap or by seeing the weakest spots on a keyboard or on a phone screen (P68)	7.4 (5)

Passcode authentication was the third most used authentication system (88.4%), and more than half the participants raised concerns (Table 8) about it. Interestingly, as well as concerns about hacking and leaks, the most frequently mentioned concern (38.2%) was that passcodes are inherently easy to crack or are less secure than passwords. This suggests that users need more information about the strength and encryption of passcodes. Some participants (7.4%) were concerned about shoulder surfing while they were entering a passcode or smudge attacks after entry. It would be interesting to investigate further how participants are aware of these issues, awareness of shoulder

surfing may well date from warnings about using automatic bank machines in public, but smudge attacks seem less well known to the public, although the phenomenon is well established [3].

Just over 40% of participants mentioned specific concerns about FIM authentication. The most frequently mentioned concern, apart from unspecified or general ones, was that FIM may be a single point of failure: if the identity provider is hacked, access may be given to a wide range of applications. The other concern is that personal information, particularly passwords may be passed to the target application. This misconception about FIM has been found in previous research [e.g. 27].

Table 9: Concerns about FIM authentication (N using = 89; N replying = 38, 42.7%)

SSO system concerns		
Single point of failure	connects accounts so if 1 is breached then they all get breached (P4)	44.7 (17)
Privacy	how secure is it? what information is being passed on (P33)	31.6 (12)
Hacking/leaks	I always use my google account to log into some sites and I feel like one day my email account will be hacked (P64)	5.3 (2)
General/Unspecified security concerns	It feels less secure, signing in through your email (P7)	18.4 (7)
SSO Use concerns		
Usability issues	Sometimes it gets messy if you already have an account and didn't realise (P42)	10.5 (4)

Nearly half the participants mentioned concerns about FaceID (Table 10), these were all about FaceID systems themselves rather than their use, suggesting that there are few usability problems with these systems. The most frequently mentioned concern was the possibility of fraudulent use of this kind of system, using AI generated face images or images stolen from the internet. Participants were also concerned that they could be forced to use the system in a robbery situation or even that someone could use it while they were sleeping. This seems an extreme concern, but perhaps participants have become of these kinds of scenarios in film, television or particularly social media. For example, there have been media reports of bank robbers conducting “digital bank robbery”, by forcing people at gunpoint to access their online account and make a transfer to the robber². The likelihood of this may be very low, but reports in the media often magnify people’s concerns about a particular situation unrealistically.

Fraudulent use was also the most commonly mentioned concern about FingerID (Table 11) and forced use was also mentioned. Usability issues were also mentioned for FingerID, mainly related to known limitations of these systems such as fingers being wet or sweaty.

² <https://www.youtube.com/watch?v=BkwKU5hdTCM>

Table 10: Concerns about FaceID authentication (N using = 72; N replying = 34, 47.2%)

FaceID system concerns		
Fraud	AI imitation being used (P114)	44.1 (15)
Forced use	If someone could force me to unlock holding it up to my face (P56) I worry that someone may use [it] .. when I am sleeping/unaware (P5)	14.7 (5)
Reliability	It sometimes doesn't recognize my face (P120)	14.7 (5)
Hack/leak	I suspect it could be hacked (P19)	8.8 (3)
Information misuse	My face ID data being exploited (P15)	5.9 (2)
General/Unspecified/ unclear security concerns	I have heard it's not as secure as using a passcode (P118)	29.6 (7)

Table 11: Concerns about FingerID authentication (N using = 61; N replying = 26, 42.6%)

FingerID system concerns		
Fraud	Someone can replicate finger print I guess? (P74)	23.1 (6)
Reliability	Not working sometimes (P126)	26.9 (7)
Forced use	Being forced by someone to log in using my fingerprint (P103)	19.2 (5)
Data theft	Theft of fingerprint (P8)	11.5 (3)
Hack/leak	Fingerprints can also be retrieved, used by other people to log in (P32)	7.7 (2)
General/Unspecified	not really sure how secure it is (P111)	30.8 (8)
FingerID Use concerns		
Usability issues	Sometimes my fingerprint won't register if my hands are too sweaty or if it's the wrong angle (P28)	7.7 (2)

FIDO authentication had the fewest participants reporting using it and also by far the fewest concerns raised. These were all in areas also affecting other authentication systems, reliability and usability, and device availability, which was mentioned for those systems which require a second device for authentication.

Table 12: Concerns about FIDO authentication (N using = 19; N replying = 6, 31.6%)

FIDO system concerns		
Reliability	Can cause problems if the card stops working suddenly, and therefore I would not be able to access my financial accounts (P61)	16.7 (1)
FIDO Use concerns		
Device availability	Losing the device or not having it when I need it (P103)	66.7 (4)
Usability issues	Annoying (P73)	16.7 (1)

5 Discussion

This study investigated the perceptions, use and concerns of a well-educated sample of British participants about seven current authentication systems. Apart from FIDO, all seven authentication systems were frequently used by a substantial percentage of the sample. This finding supports recent research [1, 5] which has found that in spite repeated statements that password authentication is dying [17], it is still very widely used. However, a number of more recent and probably more secure forms of authentication, such as 2FA and FIM, are becoming more widespread. In addition, participants rated all the systems, with the exception of FIDO, as very secure, trustworthy, and easy to use. Participants were confident about using them and generally rated their level of concern about them as low. They also thought they understood how they worked and were therefore not particularly interested in knowing more about that. The findings for FIDO were more mixed, but as this was the least frequently used system, these findings are also less reliable than the findings for the other authentication systems. When asked to express their concerns about the authentication systems, a less positive picture emerged, with many participants mentioning concerns, particularly about password authentication. This shows the importance of, whenever possible, obtaining both quantitative and qualitative data from participants in user studies.

A range of interesting issues emerged from the qualitative data, with some concerns affecting a number of the different authentication systems, for example concerns about systems being hacked, the reliability of systems, and the privacy of personal information both within the authentication systems and the information they are protecting. With password authentication, participants noted a number of the issues which have been raised in previous research [23, 31], such as difficulties remembering passwords, the tendency to therefore re-use exactly the same or very similar passwords and the need to reset passwords periodically. So, users are aware of these issues, but perhaps lack support in how to address them. It is also interesting that numerous participants expressed concerns about the security of these systems without elaborating on exactly what their concern was. This may be due to the fact that the data were collected through an online questionnaire and participants did not feel the need to elaborate, but it may also be that they genuinely cannot elaborate on what their concerns involve. Research involving interviews or focus groups, rather than a questionnaire, might be better methods for understanding more detail about the nature of people's concerns.

The qualitative data also showed that participants have misconceptions about how authentication systems work. In particular, they seem to have little awareness of the encryption of information within the systems, and that while faking fingerprints is possible, it is very difficult [19]. On the other hand, some participants were aware of smudge attacks, showing a sophisticated knowledge of authentication. A surprising number of participants had extreme concerns about the biometric authentication systems, that they might be forced to use them in a kidnap/theft situation or that someone could use their biometrics to access their online data while they slept. It would be interesting to investigate further where these particular concerns came from, whether it is an exaggeration of a very small number of incidents which have received publicity.

A number of limitations in the study need to be highlighted. For example, one reason for the apparent discrepancy between the quantitative ratings of the authentication systems and the concerns raised in the open-ended questions is that although these concerns were raised by participants, they may not be ones that concern them greatly. It may be that they are trying to be “good participants” and when asked about concerns, feel they should mention something. It would be very helpful for further research to investigate these concerns further and establish how concerned people are about them. For example, to take the specific concerns and ask people to rate their level of concern for each of them. In addition, the fact that the question about concerns for each authentication system was optional meant that very different numbers of participants answered about different systems – from 86.8% of participants who use passwords raising concerns about them, to only 31.6% of participants who use FIDO. There could be a number of reasons for this, from the fact that participants use passwords more frequently than the other systems, to the fact that genuinely fewer participants had problems with FIDO. This issue is exacerbated by the fact that FIDO was the least used authentication system with least than 15% of participants reporting using it and with low frequency, so the results from FIDO in all respects are less reliability than the other systems, which had approximately half of the participants or more reporting using them (the next least frequently used being FingerprintID with 47.3% of participants reporting using it). So all the results about FIDO need considerable further investigation.

A further limitation of the research is that the sample was a well-educated one and restricted to one country, the UK. The decision to sample from this specific population was a deliberate one, particularly in terms of restricting it to one country. The availability of different authentication systems may vary across the world, and certainly attitudes to security vary between cultures, so it was thought important to sample from a reasonably homogenous population. This also influenced the choice of a well-educated sample, although this is also a practical constraint in much research, as recruiting demographically diverse samples is difficult. However, it is perhaps the case that well-educated people in the UK are more aware of possible concerns with authentication than the general population. Again, further research is needed with more diverse samples to explore this possibility.

6 Conclusions

Overall this research has provided useful information about a range of authentication systems and highlighted a number of issues which developers and deployers of these systems need to consider in how they present them to users to address the concerns raised. It has shown that users have numerous misconceptions about how authentication systems work which may be inhibiting their adoption. Although users are aware of the security and usability issues around password authentication, this may be leading to some reluctance to wholeheartedly adopt more recent, more secure forms of authentication. It suggests that more education and more transparency in the presentation of the authentication systems would provide users with a more accurate understanding of the benefits of authentication.

References

1. Abromaityte, M., Dubero, E., Kruger, Q., et al.: Computational Analysis of User Experience of Password-Based Authentication Systems. In: Singh, D., van 't Klooster, J.W., Tiwary, U.S. (eds) *Intelligent Human Computer Interaction. IHCI 2024. Lecture Notes in Computer Science*, vol 15557. Springer, Cham. (2025).
2. Arianezhad, M., Camp, L. J., Kelley, T., Stebila, D.: Comparative eye tracking of experts and novices in web single sign-on. *Proceedings of the Third ACM Conference on Data and Application security and privacy*, San Antonio, Texas, USA. (2013).
3. Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., Smith, J. M. Smudge attacks on smartphone touch screens. *4th USENIX workshop on offensive technologies (WOOT 10)* (2010).
4. Baqeel, H., Saeed, S.: (Face detection authentication on smartphones: End users usability assessment experiences. *2019 International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). (2019).
5. Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F., Savvides, M.: Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption. *USEC '15: Workshop on Usable Security*, San Diego, CA, 1-10. (2015).
6. Bhana B., Flowerday, S.V.: Usability of the login authentication process: passphrases and passwords. *Information and Computer Security*, 30(2), 280–305. (2022).
7. Bonneau, J., Herley, C., Van Oorschot, P. C., Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *2012 IEEE symposium on security and privacy* (pp. 553-567). (2012).
8. Brostoff, S., Jennett, C., Malheiros, M., Sasse, M. A.: Federated identity to access e-government services: are citizens ready for this? *ACM Workshop on Digital Identity Management*. (2013).
9. Buckley, O., Nurse, J. R.: The language of biometrics: Analysing public perceptions. *Journal of Information Security and Applications*, 47, 112-119, (2019).
10. Ciolino, S., Parkin, S., Dunphy, P.: Of two minds about Two-Factor: Understanding everyday FIDO U2F usability through device comparison and experience sampling. *SOUPS 2019*, pp. 339-356, (2019).
11. Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., Christin, N.: "It's not actually that horrible" Exploring Adoption of Two-Factor Authentication at a University. *ACM Conference on Human Factors in Computing Systems*, pp. 1–11, (2018).
12. De Luca, A., Hang, A., Von Zeschwitz, E., Hussmann, H. I feel like I'm taking selfies all day! Towards understanding biometric authentication on smartphones. *ACM conference on human factors in computing systems* (pp. 1411-1414), (2015).
13. De Luca, A., Langheinrich, M., Hussmann, H.: Towards understanding ATM security: a field study of real world ATM use. *sixth symposium on usable privacy and security*, pp. 1-10, (2010).
14. Dutson, J., Allen, D., Eggett, D., Seamons, K. Don't punish all of us: measuring user attitudes about two-factor authentication. *IEEE European Symposium on Security and Privacy*, pp. 119-128, (2019).
15. Egelman, S.: My profile is my password, verify me! the privacy/convenience tradeoff of Facebook connect. *ACM Conference on Human Factors in Computing Systems*. (2013).
16. Furnell, S., Evangelatos, K.: Public awareness and perceptions of biometrics. *Computer Fraud and Security*, 1, 8 – 13, (2007).
17. Gates, W.H.: Keynote Presentation, RSA Conference. (2004).
18. Jones, L. A., Antón, A. I., Earp, J. B. Towards understanding user perceptions of authentication technologies. *2007 ACM Workshop on Privacy in Electronic Society*, (2007).

19. Kaspersky Daily. Faking fingerprints – doable by hard.
<https://www.kaspersky.co.uk/blog/sas2020-fingerprint-cloning/19775/>
20. Krol, K., Philippou, E., De Cristofaro, E., Sasse, M. A. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. NDSS Workshop on Usable Security, (2015).
21. Lassak, L., Hildebrandt, A. Golla, M., Ur, B.: "It's stored, hopefully, on an encrypted server": mitigating users' misconceptions about FIDO2 biometric WebAuthn. Proceedings of the 30th USENIX Security Symposium, (2021).
22. Marky, K., Ragozin, K., Chernyshov, G., et al.: "Nah, it's just annoying!" A deep dive into user perceptions of two-factor authentication. ACM Trans CHI, 29(5), 1–32, (2022).
23. Mayer, P., Volkamer, M.: Addressing misconceptions about password security effectively. 7th Workshop on Socio-Technical Aspects in Security and Trust, (2018).
24. Mihajlov, M., Jerman-Blazič, B., Josimovski, S.: A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives. 5th International Conference on Network and System Security (2011).
25. Moncur, W., Leplâtre, G. Pictures at the ATM: exploring the usability of multiple graphical passwords. ACM Conference on Human Factors in Computing Systems (2007).
26. Petrie, H., Sreekumar, G.: Passwords and single sign-on: use, security, and understanding for online accounts. 37th International British HCI Conference, (2024)
27. Petrie, H., Sreekumar, G., Shahandashti, S.: Understanding users' mental models of Federated Identity Management (FIM): use of a new tangible elicitation method. HAISA (2024).
28. Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., Seamons, K.: A usability study of five two-factor authentication methods. SOUPS 2019 (2019).
29. Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., Egelman, S.: Empirical measurement of systemic 2FA usability. 29th USENIX Security Symposium (2020).
30. Ruoti, S., Roberts, B., Seamons, K.: Authentication Melee: A Usability Analysis of Seven Web Authentication Systems. 24th International Conference on World Wide Web, Florence, Italy. (2015).
31. Shay, R., Komanduri, S., Kelley, et al: Encountering stronger password requirements: user attitudes and behaviors. Sixth Symposium on Usable Privacy and Security (2010).
32. Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., Beznosov, K. Investigating Users' Perspectives of Web Single Sign-On: Conceptual Gaps and Acceptance Model. ACM Trans. on Internet Technologies, 13(1), Article 2 (2013).
33. Theofanos, M.F., Stanton, B. C., Orandi, S. et al.: Usability Testing of Ten-Print Fingerprint Capture. Tech. Report, National Institute of Standards and Technology. (2007).
34. Tian, X. Unraveling the dynamics of password manager adoption: a deeper dive into critical factors. *Information & Computer Security*, 33(1), 117-139 (2025).
35. Volkamer, M., Gutmann, A., Renaud, K., et al. Replication Study: A Cross-Country Field Observation Study of Real World PIN Usage at ATMs and in Various Electronic Payment Scenarios. SOUPS 2018 (2018).
36. Zimmermann, V., Gerber, N.: The password is dead, long live the password—A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, 133, 26-44 (2020).