Exploring User Authentication with Windows Hello in a Small Business Environment

Florian M. Farke, Leona Lassak, and Jannis Pinter, *Ruhr University Bochum;*
Markus Dürmuth, *Leibniz University Hannover*

https://www.usenix.org/conference/soups2022/presentation/farke

This paper is included in the Proceedings of the
Eighteenth Symposium on Usable Privacy and Security
(SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

Exploring User Authentication with Windows Hello in a Small Business Environment

Florian M. Farke, Leona Lassak, Jannis Pinter, and Markus Dürmuth[‡]
Ruhr University Bochum, ‡ Leibniz University Hannover

Abstract

Windows Hello for Business is Microsoft's latest attempt to replace passwords in Windows enterprise environments introduced with Windows 10. It addresses some of the common password problems like password leaks or phishing attacks, comes with built-in support for biometric authentication methods like fingerprint or facial recognition, and a new user interface. We conducted a qualitative study with 13 employees accompanying the introduction of Windows Hello in a small business studying its usability and deployability. Over five weeks, we measured authentication times, let participants rate their user experience, and conducted interviews at the end. In general, participants liked Windows Hello and found it more usable than the traditional Windows sign-in scheme. Windows Hello was faster and perceived as more responsive than the traditional Windows login. However, participants tended to use PINs as a replacement for their (longer) passwords instead of using biometrics. Lack of hardware support (no biometric hardware available), the form factor of device or setup of their workplace (e.g., biometric hardware on the other side of the table) were some reasons to not use biometrics but stick with a well-known authentication method like a PIN.

1 Introduction

Replacing the omnipresent username and password scheme for authentication has become an ongoing quest in the usable security research community and parts of the software industry. Still, passwords are the most common approach to authenticate humans on digital devices, even though they have substantial drawbacks in terms of both usability and security: Passwords can be phished or leaked, are often reused or hard to remember, easily guessable for password-crackers, and hard to use on devices without a physical keyboard [9, 31].

Despite the weaknesses of password-based authentication only a few of the proposed alternatives found broader adoption: Graphical passwords suffer from similar drawbacks as text passwords, but are better in terms of memorability and input behavior on small touchscreens, and are used for smartphone unlocking [4, 37]. Security tokens, typically in the form of two-factor authentication (2FA), found some use in corporate contexts where setup and management of the tokens are done by an IT department or for online services with high security requirements (e.g., online banking). Regular online services usually did not offer support for these tokens because they need extra care in case of loss or theft, and in the past were often incompatible when coming from different vendors (this problem is probably solved through FIDO2[1]), and perhaps not wanted by the users [10]. Also, biometrics are not well suited for authentication at online services, as allowing the service provider to store biometric data poses a privacy and security risk to the user because biometric factors can not be changed after a data leak or when using another service. Furthermore, the provider requires access to the biometric hardware to perform the authentication.

In contrast, biometric authentication is well suited for local authentication such as smartphone unlock or sign-in on a desktop computer and can be implemented without the biometric data leaving the device. This local authentication can then be used to unlock cryptographic secrets stored in a secure enclave.

In recent years, this approach of unlocking stored login credentials was adopted in several authentication protocols (e.g., in FIDO2) and products, like for example Microsoft's Windows Hello for Business which was first introduced with Windows 10. Windows Hello for Business replaces the traditional Windows login (i.e., with username and password) with certificate-based authentication in which the private key

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

[1] https://fidoalliance.org/fido2/, as of June 9, 2022

of the user is stored locally and unlocked via facial or fingerprint recognition, security token, or PIN. Since Microsoft Windows still dominated the desktop operating systems market in 2021 (approx. 75% market share[2] of which roughly 82% was Windows 10[3]) and Microsoft's strategy of encouraging their customers to use the latest version of their operating system, we assume that Windows Hello for Business will replace the traditional Windows login in companies in the long run.

In this work, we accompanied the introduction of Windows Hello for Business in a small company, investigating the usability and perceived security of the new sign-in method. We were particularly interested in which benefits and challenges participants see when using Windows Hello and which authentication options (facial recognition, fingerprint, or PIN) they prefer to use and why. For our case study, we recruited 13 employees to voluntarily participate during their working hours. Over the course of five weeks, we followed the transition from traditional Windows authentication (with username and password or smart card) to Windows Hello for Business.

In detail, we explored the following question:

RQ1 What are the usability differences between Windows Hello for Business and the traditional Windows sign-in? *(Usability Comparison)*

RQ2 What is the perceived security of Windows Hello for Business? *(Perceived Security)*

RQ3 Which authentication options of Windows Hello for Business are people willing to adopt and why? *(Use of Biometrics)*

Our case study sheds some light on usability aspects that are important when deploying a new sign-in method and provides insights into why people adopt (or not adopt) biometric authentication in the corporate context which may also apply to contexts other than Windows Hello.

2 Background: Windows Hello for Business

With the release of Windows 10 in 2015, Microsoft introduced *Windows Hello* and *Windows Hello for Business* as new options to authenticate on a Windows computer. Both variants allow authentication using hardware tokens, biometrics (e.g., facial or fingerprint recognition), or picture passwords[4]. Text-based passwords or six-digit PINs are still available for cases in which biometric hardware is not available, is not accessible for certain user groups (e.g., people with impairments), or can not be used due to other restrictions (e.g., company policy).

As the name suggests, Windows Hello for Business integrates into Microsoft's enterprise authentication solutions while Windows Hello was designed for the consumer versions of Windows 10. Even though both variants provide the very same user interface, the inner workings and security features are quite different to meet the different use cases (i.e., authenticating via an authentication server in an enterprise network versus local authentication on a personal device). Windows Hello unlocks a password, which is stored encrypted, that is then used for authentication. In contrast to that, Windows Hello for Business is built upon public-key cryptography and uses certificates to authenticate against a remote authentication server. A Trusted Platform Module (TPM), when available, is used to securely store the login credentials and to perform cryptographic operations.

Since the login credentials are stored locally on the device and unlocked via Windows Hello, every device must be registered with a Windows account before Windows Hello for Business can be used. This binding to a device marks a paradigm shift from a knowledge-based authentication scheme (i.e., username and password) to a combination of several factors such as knowledge/biometrics and possession (i.e., the device). Such a possession-based authentication scheme is more secure because potential attackers have to gain physical control over the device instead of simply stealing the password remotely. However, requiring the use of a specific device may not be feasible for every use case, especially, for people who frequently sign in to different devices, Windows Hello for Business is not a usable solution.

3 Related Work

Windows Hello (for Business) has not been studied extensively, especially there is little research with a focus on usability. For completeness, we report the research on Windows Hello and Windows picture passwords here. However, the research is not comparable or closely related to our study. Kim et al. [22] analyzed the security of Windows Hello and propose a migration attack to compromise Windows Hello's authentication data. This attack is only applicable on devices without hardware protection. In our study, all participants used devices with TPMs where the attack is not applicable.

Issues with the Windows 8 graphical password scheme were identified by Gao et al. [17]. They studied user choices of graphical passwords in the lab and the field finding that significant hotspots exist which can be exploited in an attack.

Studying the influences of human cognition on password strength in picture passwords, Katsini et al. [21] conducted an eye-tracking study using Windows Picture Passwords. However, their goal was not to study usability or security aspects of the authentication mechanism but just used it as a working example of picture passwords for their research.

[2] https://gs.statcounter.com/os-market-share/desktop/worldwide/2021, as of June 9, 2022

[3] https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/2021, as of June 9, 2022

[4] https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview, as of June 9, 2022

Passwordless Authentication Since Windows Hello for Business is an alternative to passwords and thus a form of passwordless authentication, in the following, we discuss recent literature in this field. The FIDO2 protocols are the latest proposal for passwordless authentication. Most related in terms of methodology is a study by Farke et al. [16] in which they compared the use of security keys and passwords in a small software company. The participants found the security key to be slower than using their password manager and due to further usability issues, several employees stopped using the key despite its security benefits.

Lyastani et al. [26] compared user perceptions of passwordless FIDO2 security key logins to signing in with a site-specific password. While participants preferred the security key over passwords, the hardware-related shortcomings like account access on devices without USB ports questioned the keys' real-world suitability for passwordless authentication. FIDO2-related issues like key recovery and account revocation in case the key is lost or stolen were also mentioned.

Passwordless *biometric* FIDO2 was first studied by Oogami et al. [29] who documented the WebAuthn registration process with 10 participants on their existing Yahoo! Japan accounts. Issues with the user interface design, like a fingerprint icon being mistaken for the fingerprint reader, were identified. These results, however, are mainly relevant for the specific design of the Yahoo! Japan website.

Misconceptions about biometric FIDO2 and how to mitigate them was studied by Lassak et al. [24]. First, 42 crowdworkers used biometric WebAuthn to log in to a website and answered a questionnaire about misconceptions surrounding the login. 67% of the participants assumed that the biometric information would be transmitted to the website. In focus groups, the researchers then designed several notifications and with 345 crowdworkers investigated how they could be used to counteract users' misconceptions. The researchers found that some of the notifications partially addressed misconceptions, but misconceptions about where the biometric is stored partially persisted.

Less related but also focused on FIDO2 passwordless authentication is research by Owens et al. [30]. 97 participants logged in to a fictitious bank website over the course of two weeks with either a password or a smartphone as a FIDO2 roaming authenticator (via a prototype protocol called Neo). While Neo's security benefits were recognized by participants, login times with Neo were substantially higher than for passwords. Participants also recognized availability concerns regarding account recovery and availability of the phone.

4 Method

We designed our study to observe, in the context of a small business, the benefits employees see in using Windows Hello for Business but also what challenges they face. The employees voluntarily participated in the study using Windows Hello for Business on their work computers during their regular work time. For five weeks, we gathered sign-in data from each participant using a custom survey software application installed on the participants' work devices. Week one captured their interaction and satisfaction with their previous login method (password or smartcard). Week 2 to 5 did the same for Windows Hello. To get in-depth feedback on their experience with Windows Hello for Business, we conducted interviews at the end of the study. In the following, we outline our study protocol and explain relevant aspects of our survey application.

4.1 Study Procedure

The study procedure consists of three parts, where the second part is subdivided into two phases: (i) An initial workshop, in which we introduced the study, its procedure, and the participants' task; (ii) A five weeks long data collection phase, in which we measured authentication timings and gathered quantitative and qualitative feedback about logins consisting of: (a) One week of using a traditional password or smartcard-based login and (b) four weeks of using Windows Hello for Business; (iii) Final interviews to learn about the participants' experience using Windows Hello. An overview of the study procedure can be seen in Figure 1.

Part of the quantitative feedback was a User Experience Questionnaire (UEQ) [25]. We used the German version consisting of 26 pairs of contrasting items describing aspects of usability and user experience. These items belong to the six different categories *Attractiveness*, *Perspicuity*, *Efficiency*, *Dependability*, *Stimulation*, and *Novelty*. The only modification we performed was replacing the term *product* by *sign-in method* to fit the context of our study.

Initial Workshop To introduce our study, explain Windows Hello, and recruit participants, we invited all eligible employees to a 15-minute workshop. We began by communicating our study's purpose, procedure, and the associated risks. Since Windows Hello for Business requires to set up a PIN, we proceeded by briefing the potential participants on rules for choosing secure and memorable PINs.

By the end of the workshop, we handed out consent forms for participants to read and sign if they agreed to participate. Participation was voluntary and the entire time participants had to invest in the study took place during their working hours. In-person workshops are a typical format in which new technology is introduced in this specific company.

Using the Established Mechanism (week one) In the first week (Phase 1) of our study, we measured our baseline, with participants continuing to use their established authentication scheme (passwords or smartcards). We collected data

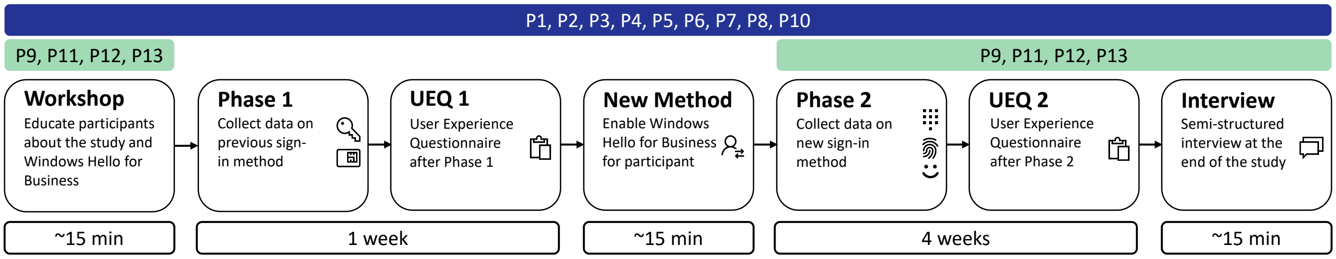

P1, P2, P3, P4, P5, P6, P7, P8, P10
P9, P11, P12, P13
P9, P11, P12, P13
Workshop
Educate participants about the study and Windows Hello for Business
Phase 1
Collect data on previous sign-in method
UEQ 1
User Experience Questionnaire after Phase 1
New Method
Enable Windows Hello for Business for participant
Phase 2
Collect data on new sign-in method
UEQ 2
User Experience Questionnaire after Phase 2
Interview
Semi-structured interview at the end of the study
~15 min
1 week
~15 min
4 weeks
~15 min

Figure 1: The study was divided into two phases: (1) The participants used the traditional Windows login for one week and filled out an UEQ afterwards; (2) They used Windows Hello for Business for four weeks and again filled out an UEQ. We conducted interviews with each participant after they finished Phase 2.

on the usage and experience with participants' previous sign-in methods via a self-developed survey pop-up we call *SurveyApp*. It automates the process of a diary study which was previously used in a paper-pencil format in similar studies [16, 23]. After every login, the SurveyApp appeared and asked the participant to rate their satisfaction with the sign-in on a five-point Likert scale. Additionally, participants had the option to add a comment. We describe the *SurveyApp* in more detail in Section 4.3. At the end of this week, participants filled in a UEQ as described above.

Using Windows Hello (week two to five) Following Phase 1, Windows Hello for Business was enabled for the participants' user accounts. To keep the changeover time as short as possible, all participants received individual assistance from the IT department during the setup. This approach ensured the best possible onboarding process and thus the satisfaction in the early study stages might reflect an upper bound. However, we think that it had little influence on the longterm usage which was our main study focus.

Once Windows Hello was successfully configured, the IT department disabled the ability to sign in with a password for the participants, leaving Windows Hello for Business as the only sign-in method available. Phase 2 was used to collect data on the usage and experience with Windows Hello for Business, in a rather normal usage context. Those participants whose devices had biometric capabilities could choose freely between authenticating via PIN or with their biometrics. Again, we collected the participants' satisfaction with the logins via our *SurveyApp* (cf. Section 4.3). This phase lasted four weeks, subsequently, participants completed a UEQ. Since users were free to choose between the different Windows Hello sign-in options, the UEQ just represents the overall experience with Windows Hello.

Interviews To gather more fine-grained feedback from the participants, we followed up with 15-minute, semi-structured, one-on-one interviews. We aimed to explore participants' impressions, feelings, and attitudes about and towards Windows Hello in more detail. The interviews were conducted and transcribed in German (see Appendix A).

We started the interviews by discussing the participants' overall perception of the new sign-in method, as well as the differences to the old, password or smartcard-based approach. For those with biometric sign-in options, we asked the participants how of they have used biometic sign-in in comparison to other sign-in options. We also asked for participants' opinions and potential general reservations towards biometrics and whether any issues occurred during the four weeks period. To compare participants' impression of authentication speed with our time measurements, we asked the interviewees to gauge how much time they usually spend per login with Windows Hello and whether this time differs from the traditional Windows sign-in. This helped us to better understand potential reasons for preferences of one or the other sign-in option. Lastly, we were interested in the participants' security perception of Windows Hello compared to their previous sign-in method. We concluded the interviews with questions about the participants' satisfaction with Windows Hello, letting them specify pros and cons, whether they would be use Windows Hello on their personal devices and if they were willing to continue using Windows Hello.

Based on the interview questions, we used an a priori coding approach to analyze the interviews [12]. The researcher who conducted the interviews created an initial set of codes using the sections of the questionnaire (see Appendix A) as themes under which one or more codes were grouped. We discussed and refined this codebook as a group to specifically focus the interview analysis on our Research Questions **RQ2** and **RQ3**. One researcher coded all 11 interviews with the initial codebook. During this coding sessions a few codes in the *Reservation Against Biometrics* Section were added We discussed the changes in the codebook and removed unused codes (e.g., the code *Password is faster* or *Prefers Fingerprint*). The revised codebook is presented in Appendix B.

Using the revised codebook, another researcher coded all interviews again. To determine the inter-coder agreement, we used the coefficient Kappa of Brennan and Prediger [7] (an improved version of Cohens' Kappa). The second coder reached a substantial agreement of $\kappa = 0.72$.

4.2 Study Environment, Recruitment, and Participants

The study was conducted at a small German company specialized in high-quality furniture, interior design, and store fitting. This environment was particularly interesting to study Windows Hello in because the needs in terms of authentication are very diverse. Employees included those in production where multiple users share a single machine, executives and sales personnel that often authenticate in public while traveling, and accountants and draftsmen who work in a regular office environment. Out of the 20 employees who regularly access computer workplaces we invited 15 to participate in our study. The remaining five were working part-time or leaving the company soon so we excluded them from our participant pool. Everyone who was invited agreed to participate. We had technical issues with the Windows Hello setup for one participant and another left the company during the study so we excluded their data from our analyses.

Due to vacation or sickness, the study start and end dates of the participants varied. The total time frame for the entire study ranged from August 2021 when we held our initial workshop to November 2021 when our last participant was interviewed. The study was conducted during the Covid-19 pandemic, however this did not specifically influence the study environment or work flows in the company at that time.

Before the study, all except four participants had only used passwords or smartcards to sign in at their workplace. The four other participants had been part of a pilot test of Windows Hello that had been carried out by the company before our study. This pilot test solely tested the migration from passwords to Windows Hello from a technical perspective and was independent from our study. Since they already had three to four months of experience with Windows Hello, they did not participate in Phase 1 of the study as it would have been confusing to switch them back to passwords just for the purpose of the study.

Demographics Out of the 15 eligible employees, 13 participated. Out of these, five were women and eight were men. 40% were aged between 18 and 29, 20% between 30 and 49, and 40% were 50+. None of the participants had a background in IT. Participants' job positions ranged from Engineering and Design over Production Planning to Administration and Executive.

Computer Hardware and Password Policy The computer hardware of our participants varied in terms of model and also authentication capabilities. Most computers were Lenovo machines including different models of the *ThinkStation*, the *ThinkCentre*, and the *ThinkPad*. Other participants used a Microsoft Surface Pro 7+. All 13 computers had a built-in TPM and could be unlocked via PIN. Additionally, four out of the 13 machines had a fingerprint reader, 3 offered fingerprint and face recognition, and one offered only face recognition. During the study, all computers ran on Windows 10 Professional with build number 19043 (21H1), which was the latest release of Windows 10 at that time. The machines received monthly security updates by Microsoft, but no feature updates were installed during the time of the study to obviate issues as much as possible. Per the company's policy, all computers are locked automatically after 10 minutes of inactivity.

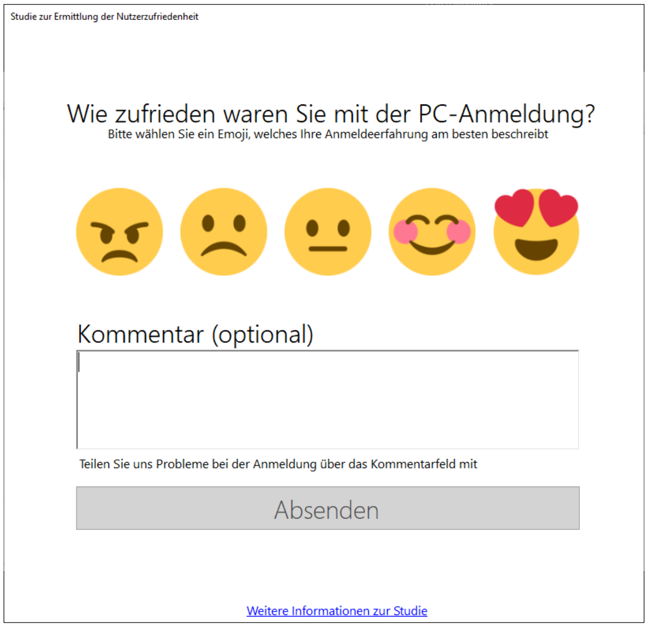
The company's password policy only specified a length of at least 10 characters. Further complexity requirements such as the use of upper/lower case letters, numbers, or special characters were not specified. Also, the company did not enforce regular password changes.

4.3 Implementation

SurveyApp To collect satisfaction ratings from our participants continuously during the entire period of the study, we developed a GUI application (which we call *SurveyApp*). It was displayed immediately after every sign-in the participants performed even before the actual desktop screen was shown, and participants could rate their experience on a 5-point emoji scale (cf. Figure 2). We chose emojis for their intuitive meaning and quick interaction [1]. To unify the interface and prevent misinterpretation due to differing renderings on different machines [27], we displayed the emojis as images. To further prevent misinterpretation, each emoji was equipped with a tooltip showing the satisfaction level as text, they were displayed in ascending order, and explained during our initial workshop. The SurveyApp also provided the option to submit voluntary comments which was, however, barely used by our participants.

Time Measurements To our knowledge, no Windows API exists that provides data on the authentication of a user, specifically the exact time frame when the user first starts the sign-in to when the authentication is finished. The Microsoft Windows lock screen *LogonUI* changes memory consumption deterministicly depending on the user interaction. For example, dismissing the lock screen and the submission of credentials can be seen as separate events in the memory traces. An example of such a memory trace can be seen in Appendix C. We decided to use the memory profile as a side-channel to measure the authentication timings. To capture all sign-ins, our background application periodically checks the process table for a running LogonUI process and when it is present, records the processes' memory usage every 250 milliseconds. Since it is unlikely that a sign-in takes longer than 60 seconds and to limit the memory footprint of the background service itself we only preserved the last 60 seconds of memory usage data.

We are aware that these timings are not entirely accurate since users, e.g., might dismiss the lock screen by accident



Studie zur Ermittlung der Nutzerzufriedenheit

Wie zufrieden waren Sie mit der PC-Anmeldung?

Bitte wählen Sie ein Emoji, welches Ihre Anmeldeerfahrung am besten beschreibt

Kommentar (optional)

Teilen Sie uns Probleme bei der Anmeldung über das Kommentarfeld mit

Figure 2: After each sign-in, the SurveyApp showed a window in which the participants were asked how satisfied they were with the login procedure. To answer the question, participants had to click one of the five emojis and the submit button (in German: "Absenden"). Optionally, participants could give additional feedback via the text field.

when not actually attempting a sign-in. Or its possible that some time between dismissing the lock screen and sign-in is not dedicated to authentication but might be spent talking to a colleague coming by. Since in our study our main interest surrounds the question of which method is faster and the limitations apply to passwords and Windows Hello authentication equally, we consider this method valid to answer our question. In short: it is important to acknowledge that our time measurements are a valid means of comparing authentication timings *within the scope of our study* but they *are not* an accurate representation of *actual* login times. LogonUI also provides information on the used sign-in method which allowed us to identify whether PIN or a biometric sign-in was used during the Windows Hello phase.

Timing Data Analysis A challenge in the analysis of the timing data we captured via the memory consumption "sidechannel" is the fact that the individual memory profiles differ on each machine and depend on the specific environment. For example, on some machines LogonUI's memory usage increases when the screensaver is disabled while on others the memory usage decreases. These slight differences make it difficult to automate the evaluation of sign-in timing data. Additionally, specific memory profiles, like the first sign-in after the machine has booted do not follow the typical memory profile pattern. For our timing data analysis we therefore apply manual post-processing instead of an automated analysis. From the entire data set, we randomly sampled time measurements and ensured that a similar amount of timing data was analyzed for each participant. In total, we selected and analyzed 66 time measurements of the 226 sign-ins from Phase 1 and 244 time measurements of 1,419 sign-ins from Phase 2.

4.4 Ethical Considerations

Our institution does not have an ethics board governing such types of studies. We made sure to follow ethical principles laid out in the Belmont report [28] and discussed the study's ethical perceptive with peers. We collected our participant's informed consent emphasizing that not participating or withdrawing from the the study later on would not include any negative consequences for them; neither personally nor for their work. We made sure to reiterate this information during every new phase of the study. We acknowledge that the involvement of the employer in this study might pose more pressure on subjects to participate, fearing negative consequences for their regular work. To minimize this effect we repeatedly emphasized how no negative consequences would occur even if participants withdrew their consent. Moreover, we thoroughly ensured that participants were aware that their sign-ins are monitored during and only during the time frame of the study. Participants did not receive any explicit compensation because the study took part entirely during their normal working hours so they did not have any additional effort or workload. Participants' data was pseudonymized before analyzing and publishing the results. Basic data protection measures such as encrypting the data in transit and access controls were applied to reduce the risk of a breach.

4.5 Limitations

We did an exploratory study of Windows Hello for Business in a small company in Germany and due to the qualitative nature of the study, real-world setting, and the size of the company, we could only recruit 13 participants (which, nevertheless, is representative for this company). As four of the participants already used Windows Hello before we conducted the study, we could not collect the same data of their use of the traditional Windows login as for the other participants. Another participant (P5) used a smart card instead of a password for sign-in, which is a very different authentication method that does not allow a direct comparison. All these factors led to a small and heterogeneous sample. Thus, study results are not generalizable to other authentication settings or companies. Especially, the data on use of biometrics is very limited and does not allow in-depth comparisons or to draw conclusions for other environments. The specific workplace setup also influenced the specific outcomes in preferences and authentication choices and is not representative for different types of companies. Nevertheless, we consider the setup quite common for office and stationary desk focused workplace settings. The company culture appeared fairly trusting which might have had a positive influence on the participants' openness to changes so results are closely related to trust, especially biometrics usage, should be interpreted carefully and rather considered as an upper bound.

Moreover, as mentioned above, our time measurements and analysis methodology do not allow statements about real-world authentication timings but only comparisons within the scope of our study.

5 Results

We structured this section along our research questions. First, we show the results concerning the usability differences of Windows Hello for Business and the traditional Windows login. Secondly, we present our findings on the perceived security of Windows Hello. Finally, we illustrate why participants used or not used Windows Hello with biometrics. To provide context to the data that we gathered via our SurveyApp, we present a brief summary of the number of sign-ins we used in our analysis.

Frequency of Sign-ins Through the SurveyApp, we measure 226 sign-ins performed by the nine participants of Phase 1 and 1,419 uses of Windows Hello for Business in Phase 2 of the study. On average, each participant performed between 28 and 29 sign-ins via Windows Hello per week (*SD*: 10.8). However, due to different work routines, the number of sign-ins greatly varies among the participants and over the course of the study since some participants went on vacation or got sick. Participant P5 had much fewer sign-ins (30 in total) than all other participants, because they were a trainee and attended school two days per week. During the four-week period, P13 performed the most sign-ins with a total of 203 logins. Figure 7 in Appendix C shows the frequency of sign-ins of the participants in more detail. A more detailed description of the usage of different biometric methods can be found in Section 5.3.

5.1 RQ1: Usability Comparison

To explore our first Research Question **RQ1**, we used the results from the UEQs, the time measurements and ratings from the SurveyApp, and the responses from the interviews. As participants P9, P11, P12, and P13 already used Windows Hello before the study, we could not gather bottom-line data (i.e., login times, satisfaction ratings, and UEQ for the traditional Windows login) for these participants. We also excluded results of participant P5 from the UEQ comparison because they used a smartcard instead of a password. However, we explicitly asked all participants in the interviews to compare Windows Hello for Business with the authentication method they used before.

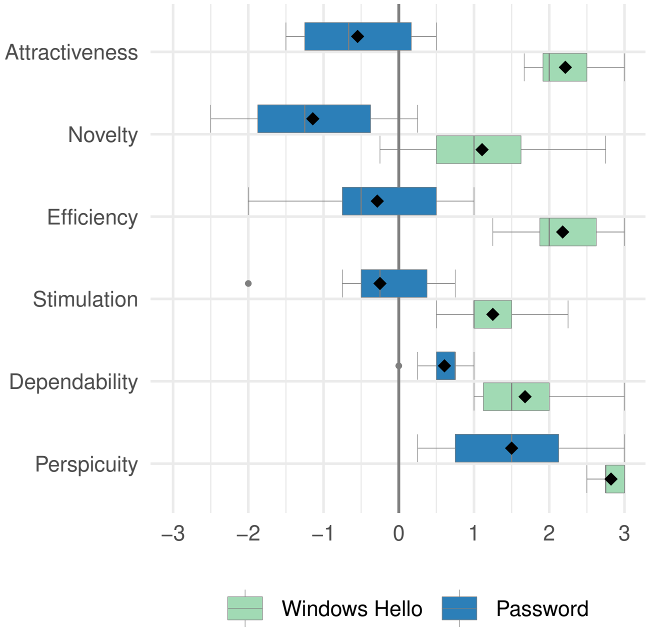


Figure 3: UEQ results for each of the six categories after the first phase (Password) and the second phase (Windows Hello). All boxes for Windows Hello are on the positive side of the scale, indicating an excellent usability experience. In contrast, ratings for password are more skewed to the negative side of the scale.

Usability Experience Questionnaires The evaluation of the UEQs showed that Windows Hello for Business scored better than the password-based Windows login across all six UEQ scales. As mentioned before, we only used the responses from the participants that originally used passwords (P1, P2, P3, P4, P6, P7, P8, and P9) for the comparison shown in Figure 3.

Windows Hello was rated particularly well on the *Perspicuity*, *Attractiveness*, and *Efficiency* scales with average scores higher than two. These high ratings indicate that Windows Hello is even easier to understand than passwords (which also receive fairly high ratings on the Perspicuity scale) while being much more attractive and efficient to use than passwords. Overall, the UEQ ratings for Windows Hello were all *above average*, most of them even *excellent*, compared to the UEQ benchmark data set [36]. In contrast, the ratings for the password-based login are considered as *bad*, except from Perspicuity which was rated *above average*. Comparing the UEQ results of password-based authentication and Windows Hello via t-tests (as described in the UEQ handbook [35]) reveals significant differences for *Attractiveness*, *Efficiency*, *Stimulation*, and *Novelty* scales ($p < 0.01$). The test results for *Perspicuity* and *Dependability* ($p < 0.02$) are almost significant. Table 1 gives an overview of the UEQ results of the two sign-in methods and puts them in relation to the benchmark data set.

Table 1: Comparison of UEQ results for password-based Windows login and Windows Hello for Business with the UEQ benchmark dataset [36] and paired t-test for each scale [35]. The results were corrected via Bonferroni–Holm method.

	Password		Windows Hello		t-test	
Scale	**Mean**	**Benchmark**	**Mean**	**Benchmark**	**t**	**Pr(>|z|)**
Attractiveness	-0.56	Bad	2.21	Excellent	-8.86	<0.001 ***
Novelty	-1.25	Bad	1.06	Good	-4.76	0.001 **
Efficiency	0.00	Bad	2.16	Excellent	-4.41	0.003 *
Stimulation	-0.41	Bad	1.19	Above Avrg.	-3.98	0.003 *
Dependability	0.75	Bad	1.66	Excellent	-2.89	0.015 ·
Perspicuity	1.69	Above Avrg.	2.84	Excellent	-2.97	0.019 ·

Signif. codes: *** ≙ < 0.001; ** ≙ < 0.01; * ≙ < 0.05; · ≙ < 0.1

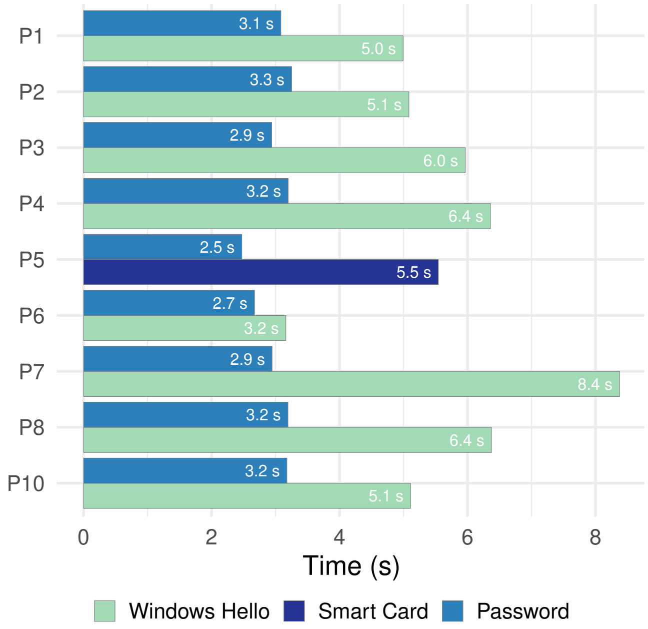


Figure 4: Average sign-in duration per participant and sign-in method. Windows Hello for Business was faster for each participant.

Authentication Speed Comparing the sign-in timings, Windows Hello for Business was faster for all participants in the study. The sign-in times for password ranged from 3.2 s (P6) to 8.4 s (P7), that is 5.7 s on average. For Windows Hello, the sign-in took 2.5 s (P5) to 3.3 s (P2 and P10), on average 3.0 s. These results indicate that authentication with Windows Hello was on average 47% faster than password-based authentication. Figure 4 shows the differences in the duration of the sign-in process between password authentication and Windows Hello for each participant.

When we asked the participants in the interviews which aspect of Windows Hello for Business they liked the most, all of them mentioned the faster authentication speed.

> *Definitely, happier than with the password, because it's simply faster.* (P8)

This finding suggests that the usability of Windows Hello greatly benefits from the gain in authentication speed. Some participants attributed the speed gain to the shorter PINs.

> *Faster, because the PIN is obviously shorter than my old password.* (P11)

Previously, participants used passwords of a length of at least 10 characters. The new PINs consist of 6 digits for all participants. Many participants reported that they used long and complex passwords which were hard to remember while the PINs are easier to remember.

> *With the password, well I've used, I think, a 16-character password consisting of upper/lower case letters, numbers, and special characters. Once you've learned it by heart, than it's fine but if you have to learn a new one then it takes some time to memorize it. A six-digit PIN is easier to learn.* (P7)

Although, we did not measure authentication errors, the error-rate is another factor influencing the authentication speed and participants mentioned this aspect during the interviews.

> *I mistype less, as with upper/lower case letters and such, because it was just numbers.* (P4)

Windows Hello also requires less interaction during the authentication procedure than the traditional login. Instead of waiting for confirmation after entering a PIN by clicking a button on the user interface or pressing Enter, Windows Hello tries to perform a sign-in after the correct number of key strokes. Participants noticed this subtle difference between PIN entry and the traditional password entry and saw it as a benefit.

> *I don't have to press enter, so it's a bit faster.* (P7)

Another improvement of Windows Hello is that it ignores the state of Num-Lock and always allows to enter numbers on the number keypad.

> *I don't have to check the keyboard, I can type right away, even if that number light isn't on, it still worked, I liked that.* (P4)

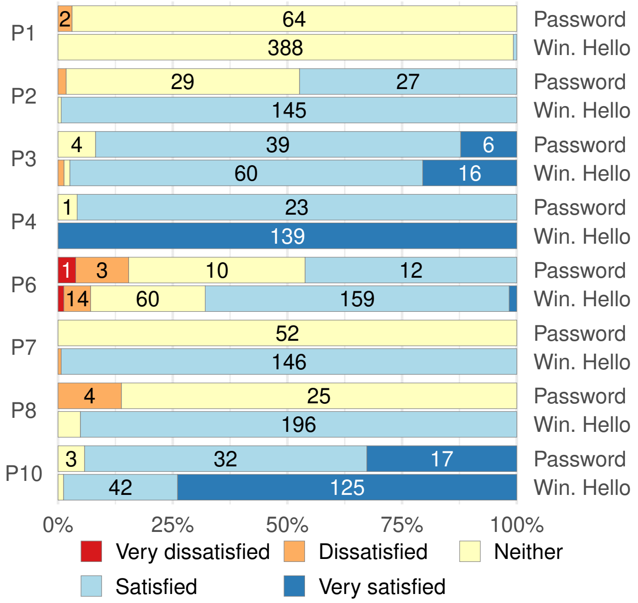


Figure 5: Satisfaction ratings submitted via the SurveyApp after each sign-in grouped by authentication method and participant. Only participants using passwords in Phase 1 are included in the bar chart. The numbers on the bars are the absolute number of ratings per level of satisfaction.

This improvement also helps to avoid errors and thus increases the authentication speed. One participant stated that fingerprint recognition annoys her and that she prefers to sign-in with her PIN because she feels it is faster and she already has her hands on the keyboard.

> *No, fingerprint annoys me. If I don't put my finger correctly on the reader, I can sign-in faster with the PIN, also because I can type quickly. In short, fingerprint makes me uncomfortable and I already have my fingers on the keyboard anyway.* (P9)

Satisfaction Beside the time data that we gathered, we asked the participants after each successful sign-in how satisfied they were with it via the SurveyApp (see Section 4.3 and Figure 2). Figure 5 shows the satisfaction rating for the eight password-using participants.

Overall, most of the ratings were positive or neutral and participants ratings were mostly consistent over time (Participant 6 being an exception). However, the ratings for Windows Hello tend to be higher than for password-based authentication. which is also confirmed by a Wilcoxon signed-rank test ($p < 0.01, V = 0$). We used a Wilcoxon signed-rank test since we could not assume equidistance for our satisfaction items. The higher satisfaction with Windows Hello is in line with our findings from the UEQs and the feedback from the interviews.

5.2 RQ2: Perceived Security

In general, the participants were not aware of any of the security features that Windows Hello for Business offers. However, the perceived security of the different sign-in options provided by Windows Hello varied greatly among the participants.

Facial Recognition When asked which of the three sign-in options (i.e., facial recognition, fingerprint, PIN), eight participants found facial recognition to be the most secure. Participants trusted facial recognition more than fingerprint recognition, for example, they argued that the facial recognition software were more sophisticated, that it would involve several features of the face, and were resistant to simple forgery attacks.

> *I'm not an expert in this area but I imagine that facial recognition software can store several features, eye distance, face shape, etc., and that this may be even more secure than a PIN.* (P2)

> *Perhaps facial recognition is even more secure, we tested it once, with a photo and via FaceTime, neither was accepted by the system.* (P10)

Fingerprint Recognition One participant stated that fingerprint recognition is the most secure sign-in method but could not explain why.

> *I think fingerprint is probably even more secure than facial recognition. But it's just a feeling.* (P6)

PIN Another participant said PIN is the most secure sign-in method, explaining that they did not trust the technology and that one can make up their own PIN which would be hard to guess.

> *I don't know. Sometimes I don't trust things, you come up with a PIN yourself, it's hard to steal but I don't know if there isn't a vulnerability, especially with the camera and the facial recognition, I'm not so sure.* (P5)

Biometrics in General Participant P9 considered both biometric sign-in options more secure than PIN, but saw no difference between facial recognition and fingerprint in terms of security.

> *Fingerprints are not used without reason as a unique identifier in identity documents, so in this respect I think that such a fingerprint is really secure. But basically, facial recognition and fingerprints are equally secure.* (P9)

Windows Hello for Business in General Participant P11 stated that all options of Windows Hello were equally secure. They explained in the interview that facial recognition and fingerprints are more secure than a password. When asked whether the PIN was more secure, less secure, or equivalent to the biometric methods, the participant said the PIN was equivalent to the biometric methods.

Passwords One participant considered facial recognition to be less secure than PINs and would prefer to not use it for more critical services like online banking.

> *I don't think I'd do my online banking with facial recognition now, because I just don't know enough about it, and if someone can fool it with photos or whatnot.* (P7)

Instead, the participant considers a long, complex password with upper/lower case letters, numbers, and special characters to be the most secure.

> *A 16 character password with special characters, upper/lower case letters, and numbers seems more secure to me.* (P7)

The participant has previously read up on secure passwords and learned that complex passwords are harder to guess than less complex ones.

> *So, I was on a password test site where I can enter a password, and the site tells me how long it would take a computer to hack it. When I use a longer, more complex password and more different character types, then it displays that it takes a million years to hack it.* (P7)

However, guessing attacks are only one problem and phishing or password reuse are still problematic even if a complex password is used. This statement underlines, why security literacy is an important factor when deploying a new security feature since it helps people to better understand the change and may increase acceptance.

5.3 RQ3: Use of Biometrics

As described in Section 4.2, only eight participants had devices with biometric hardware compatible with Windows Hello (cf. Section 4.5). We encouraged these eight participants to try and use the different sign-in method available on their devices when Windows Hello was enabled in the beginning of Phase 2. Besides a PIN, which every participant could use, Participants P6, P7, P8, and P9 could use facial and fingerprint recognition. Participants P10, P11, and P12 had only fingerprint readers on their devices and P13 had a face recognition camera available.

However, our results show that only two participants frequently used the biometric sign-in option. Participant P13 used facial recognition most of the time (174 out of 203 logins; 86%), and P11, who used facial recognition sometimes (21 out of 112; 19%). All other participants (almost) always used PINs for authentication via Windows Hello. Using PIN instead of biometric authentication is counter-intuitive as people usually find biometric authentication more secure than passwords or PINs [38].

5.3.1 Reasons Not to Use Biometrics

Influence of Workplace Setup While our participants did use laptops as work stations, these were mostly used with external screens and docking stations. The laptops were often placed on the far side of the desk with closed lid and hard to reach. This prevented easy access to the fingerprint scanner which was mostly located next to the laptop keyboard. Similarly, the built-in cameras were located at the top or bottom of the laptop display. Opening the laptop lid for each sign-in cancels out the convenience that biometrics may have because it requires additional steps and thus protracts the sign-in. We also found that for facial recognition, the angle and distance at which the laptop was placed to the user highly influenced the accuracy and success rate of the logins.

> *Maybe it's because the computer is too far away. About a meter on the right side and I have to face at my laptop, so to speak, and then sometimes it does not recognize me.* (P12)

Participant P13, who used facial recognition most frequently, had a different setup than P12. They used a convertible device where the docking station is connected via a cable instead of a fixed mount. In order to use the device it also cannot be closed but must sit in an upright position. These factors address the exact issues mentioned by Participant P12; a closed laptop lid, a laptop positioned too far away, and at the wrong angle. Participant P13 had the flexibility to place the device closer and change the angle in which the device is directed towards them which could explain their more extensive facial recognition usage.

Fear of Being Observed Four participants (P9, P10, P11, and P12) reported a feeling of being watched by the camera and preferred, for this reason, the PIN sign-in option.

> *With facial recognition, you're always a bit more skeptical, the camera is always on, and you've heard stories that they can be hacked.* (P11)

Participants who already used facial recognition sporadically were asked if they would use facial recognition more often if they had a camera not only on their laptop, but also on their main screen, which would be better oriented toward them and could eliminate the workplace setup issues discussed above. All three of these participants (P10, P11, and P12) expressed their discomfort with the idea of having a camera mounted on top of the main display.

> *But then I might feel like I'm being watched.* (P10)

On the contrary, other participants suggested that mounting an external camera on top of the primary monitors could be a could solution to workplace setup issues.

Fear of Being Locked Out Three participants (P2, P4, P11) saw risks regarding availability if there were technical problems with facial or fingerprint recognition. While those participants did not consider their fear as a reason not to use biometric authentication, they did emphasize the importance of having the PIN at least as a fallback option. Specifically, they feared that the camera could break or fail to recognize them if features in their face changed.

> *Face recognition always requires a working camera. Does it work when I shave off my beard? I don't know if it still works then, no clue.* (P11)

5.3.2 Reasons to Use Biometrics

Most participants did express to not have a general aversion against biometrics. Participant P3, for example, stated that they also use fingerprint recognition on their personal laptop. All five participants that used a PC without biometric capabilities mentioned that they would use biometrics if it were available on their PC, as well. Participant P13, who used facial recognition regularly, underlines this positive attitude towards biometrics, describing it as easier to use.

> *And with facial recognition, it's just a much easier recognition.* (P13)

A situational preference for biometrics was described by participant P12. Overall, they preferred the PIN for the aforementioned reasons but used facial recognition in situations where other people are present in the same room or behind them when signing in. The participant deliberately used facial recognition to avoid other people being able to see their PIN when they entered it.

> *I have both options, if I wish that no one can see my PIN, then I just go to the camera, then I do not have to enter anything. I can decide freely.* (P12)

Arguments for fingerprint and facial recognition, that are also commonly described in biometric authentication literature [3, 11] were also mentioned by a number of participants, for example, that facial recognition does not require anything to be remembered, since it does not require entering a secret. While this a valid statement, it should be noted that Windows Hello for Business always falls back to the six-digit PIN when facial or fingerprint recognition does not work (e.g., when the camera is disconnected or the lighting conditions have changed). Therefore, there is a risk that users will sign-in exclusively with biometrics over an extended period of time and then tend to forget their PIN over time, which would potentially lock them out of their device when the biometric recognition fails.

6 Discussion

Studying usability in the field instead of a lab or online setting helps to better understand what works well of, in our case, Windows Hello for Business and what obstacles people encounter when using it on a daily basis. In our study, Windows Hello for Business outperforms the traditional login in most usability aspects. We found that the Windows Hello login is on average 47% faster than the login with passwords. This is also reflected in the employees' satisfaction with the new authentication mechanism.

Knowledge-based Authentication vs. Biometry Usually, passwords are not very popular among users and suffer from various well-studied usability and security issues [9, 20, 31]. In recent years, a multitude of efforts have tried to counteract and overcome the password issues, trying to populate the use of password managers [15, 32], graphical authentication [4, 37], and Multi-factor authentication [19, 33, 34] are just a few to mention in this list. Biometric authentication has been one of the few approaches that have proven to be a viable, accepted, but still secure alternative to knowledge-based authentication – at least in certain authentication contexts [18]. Our results offer interesting insights into relevant factors for the real-world adoption of biometric authentication in the context of a corporate environment. Contrary to most findings in the literature, where users prefer biometric authentication over knowledge-based variants [3, 11], in our study, most participants resorted to using knowledge-based authentication (PINs) instead of biometrics. While participants in our company worked mostly stationary, this is different in other work settings especially for those traveling to customers and working on the go. One of our participants mentioned resorting to face recognition whenever someone was present nearby to prevent shoulder surfing. Compared to passwords, where shoulder surfing in public places in inevitable, the biometric option in Windows Hello allows for shoulder surfing prevention while on the go.

Recommendation: *Companies considering a switch to Windows Hello should take their employees work modalities into account. For example, by only providing biometric hardware for those in need of shoulder surfing protection.*

Next, we discuss factors that played a role in participants' decision to use PINs instead of available alternatives.

Both *hardware availability* and *hardware placement* played an important role in participants' decisions against biometric authentication. As described in Section 5.3, the participants mostly worked with external displays and docking stations for laptops. This is typical for office settings, where laptops are placed outside of direct reach, and lids are kept close. Consequently, built-in fingerprint readers are not (easily) accessible, and the built-in cameras are either not facing the user, or facing users from angles they typically are not looking at. Furthermore, lock screens are typically displayed on the main display, which often is not the one with the camera, making face unlock awkward to use. This is in sharp contrast to authentication on mobile devices, where biometrics have a significant share (e.g., 80% consumer devices in the USA had biometrics enabled in 2020 [13]). Here, the sensors for fingerprint and face recognition are placed to be reachable easily when using the device.

Recommendation: *Biometric hardware can offer great usability benefits but only in the correct usage setting. If it is not essential for a company to offer biometric logins it can be sufficient to offer Windows Hello with PINs since high user satisfaction can be expected.*

Privacy Issues While in recent years, most of the laptops and convertibles come with built-in facial or fingerprint recognition capabilities, in office environments stationary computers are still broadly used which do not have these functionalities built-in (five participants had such a device). The aforementioned workplace setup can render some of the built-in authentication hardware useless. Consequently, additional hardware for biometric authentication needs to be purchased and set up which is an investment that some employees potentially disprove, either because they do not want to use their fingerprints for authentication at work or feel under surveillance when facial recognition cameras are mounted to their displays. Such *privacy-related concerns* with using biometrics are well-known in the literature [8] but have more severe implications in the corporate context than for private usage. The company we conducted our study at was a small, family-owned business with a trusting work climate so our participants did not strongly express any explicit privacy concerns with regard to their company. However, this might be different in larger corporations or in less positive work climates, especially in cases where employee surveillance has already been an issue [2, 5, 14]. In those cases, employees might feel like their privacy is invaded when being encouraged or even enforced to use biometrics. Facial recognition can even evoke a feeling of being monitored. Part of the solution could be the use of cameras with built-in shutters. However, since even PINs were highly accepted, more usable, and much faster than the traditional Windows sign-in, it might be sufficient to rely on non-biometric Windows Hello.

Recommendation: *When choosing (biometric) hardware for Windows Hello take your company culture and trust environment into account to obviate employees feeling uneasy or even monitored. For some companies it might be sufficient to rely on PINs and not introduce biometric hardware after all.*

Deployment of Windows Hello Even though Windows Hello offers some strong usability benefits (like *Quasi-Memorywise-Effortless*, *Quasi-Physically-Effortless*, *Easy-to-learn*, *Efficient-to-Use*; cf. Bonneau et al. [6]) it introduces extra effort in the deployment phase (*Negligible-Cost-per-User* not fulfilled). As the login credentials of Windows Hello are tied to a specific device, i.e., every device, a person wants to use, has to be enrolled with the Windows account of that person (cf. Section 2). In organisations in which people share their devices, the default setup of Windows Hello for Business, i.e., using the built-in TPM, is not feasible.

Smartcards or other hardware tokens (e.g., FIDO2 tokens like YubiKeys[5]) have the advantage that they support roaming. The same goes for passwords which are stored with the user account on a server in the enterprise's network and not on the individual devices.

However, the authentication secret being bound to and never leaving the device is an intentional security and privacy-preserving feature of Windows Hello. This might not be an issue or even beneficial in work environments where every user has their own device and only uses that but in many work settings with several shared computers, Windows Hello will not provide the necessary flexibility a password or roaming token does.

Recommendation: *Windows Hello using the built-in TPM is less suited for shared devices, especially with many users. Relying on roaming authenticators or the traditional password is a better choice in these cases.*

7 Conclusion

We studied Windows Hello for Business, Microsoft's latest alternative to traditional password authentication. In a small business, we measured authentication times of 13 employees, collected their experience, and conducted interviews to understand their perceptions of and attitudes towards Windows Hello in the wild. Our five weeks long study revealed that, in general, participants like Windows Hello, finding it more usable than the traditional Windows sign-in methods. Windows Hello was measurably faster, perceived as more responsive, and convenient to use. Contrary to findings on biometrics usage in mobile devices, participants in our study tended to use PINs most of the time. This was partially due to a lack of availability of biometric hardware, the form factor of their device, and the setup of their workplace (e.g., biometric sensor not reachable).

Acknowledgment

This research was partially funded by the MKW-NRW research training group SecHuman and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972.

[5] https://www.yubico.com/products/yubikey-5-overview/, as of June 9, 2022

References

[1] Sarah Alismail and Hengwei Zhang. The Use of Emoji in Electronic User Experience Questionnaire: An Exploratory Case Study. In *Hawaii International Conference on System Sciences*, pages 3366–3375. ScholarSpace, 2018.

[2] Raluca Balica. Automated Data Analysis in Organizations: Sensory Algorithmic Devices, Intrusive Workplace Monitoring, and Employee Surveillance. *Psychosociological Issues in Human Resource Management*, 7(2):61–66, 2019.

[3] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywey, Lorrie Faith Cranor, and Marios Savvides. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In *Workshop on Usable Security*. ISOC, 2015.

[4] Robert Biddle, Sonia Chiasson, and Paul C. Van Oorschot. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys*, 44(4):19:1–19:41, 2012.

[5] Stephen Blumenfeld, Gordon Anderson, and Val Hooper. COVID-19 and Employee Surveillance. *New Zealand Journal of Employment Relations*, 45(2):42–56, 2020.

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

[7] Robert L. Brennan and Dale J. Prediger. Coefficient Kappa: Some Uses, Misuses, and Alternatives. *Educational and Psychological Measurement*, 41(3):687–699, 1981.

[8] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. On the Impact of Touch ID on iPhone Passcodes. In *Symposium on Usable Privacy and Security*, pages 257–276. USENIX, 2015.

[9] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security*. ISOC, 2014.

[10] Sanchari Das, Andrew Dingman, and L. Jean Camp. Why Johnny Doesn't Use Two Factor: A Two-Phase Usability Study of the FIDO U2F Security Key. In *Financial Cryptography and Data Security*, pages 160–179. Springer, 2018.

[11] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In *ACM Conference on Human Factors in Computing Systems*, pages 1411–1414. ACM, 2015.

[12] Jessica T. DeCuir-Gunby, Patricia L. Marshall, and Allison W. McCulloch. Developing and Using a Codebook for the Analysis of Interview Data: An Example from a Professional Development Research Project. *Field Methods*, 23(2):136–155, 2011.

[13] Duo Security. The 2020 Duo Trusted Access Report: A Remote Access Playbook, March 2021. https://duo.com/resources/ebooks/the-2020-duo-trusted-access-report, as of June 9, 2022.

[14] Lilian Edwards, Laura Martin, and Tristan Henderson. Employee Surveillance: The Road to Surveillance is Paved with Good Intentions. In *Amsterdam Privacy Conference*, pages 1–30, 2018.

[15] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. An Investigation Into Users' Considerations Towards Using Password Managers. *Human-Centric Computing and Information Sciences*, 7(1), 2017.

[16] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Symposium on Usable Privacy and Security*, pages 19–35. USENIX, 2020.

[17] Haichang Gao, Wei Jia, Ning Liu, and Kaisheng Li. The Hot-Spots Problem in Windows 8 Graphical Password Scheme. In *Symposium on Cyberspace Safety and Security*, pages 349–362. Springer, 2013.

[18] Rachel L. German and K. Suzanne Barber. Consumer Attitudes About Biometric Authentication. Technical Report UT-CID-18-03, The University of Texas at Austin, May 2018.

[19] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M. Redmiles. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *USENIX Security Symposium*, pages 109–126. USENIX, 2021.

[20] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *ACM Conference on Computer and Communications Security*, pages 1549–1566. ACM, 2018.

[21] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. Influences of Human Cognition and Visual Behavior on Password Strength during Picture Password Composition. In *ACM Conference on Human Factors in Computing Systems*, pages 87:1–87:14. ACM, 2018.

[22] Ejin Kim and Hyoung-Kee Choi. Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild. *Security and Communication Networks*, 2021(1):6245306:1–6245306:13, 2021.

[23] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *Workshop on Usable Security*. ISOC, 2015.

[24] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *USENIX Security Symposium*, pages 91–108. USENIX, 2021.

[25] Bettina Laugwitz, Theo Held, and Martin Schrepp. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work*, pages 63–76. Springer, 2008.

[26] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy*, pages 268–285. IEEE, 2020.

[27] Hannah Jean Miller, Jacob Thebault-Spieker, Shuo Chang, Isaac Johnson, Loren Terveen, and Brent Hecht. "Blissfully Happy" or "Ready to Fight": Varying Interpretations of Emoji. In *International Conference on Web and Social Media*, pages 259–268. AAAI, 2016.

[28] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, September 1978. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html, as of June 9, 2022.

[29] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. Poster: Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones. In *Symposium on Usable Privacy and Security*. USENIX, 2020.

[30] Kentrell Owens, Blase Ur, and Olabode Anise. A Framework for Evaluating the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Who Are You?! Adventures in Authentication Workshop*, pages 1–5, 2020.

[31] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. Beyond Credential Stuffing: Password Similarity Models using Neural Networks. In *IEEE Symposium on Security and Privacy*, pages 866–883. IEEE, 2019.

[32] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why People (Don't) Use Password Managers Effectively. In *Symposium on Usable Privacy and Security*, pages 319–338. USENIX, 2019.

[33] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A Usability Study of Five Two-Factor Authentication Methods. In *Symposium on Usable Privacy and Security*, pages 357–370. USENIX, 2019.

[34] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent E. Seamons. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *IEEE Symposium on Security and Privacy*, pages 872–888. IEEE, 2018.

[35] Martin Schrepp. User Experience Questionnaire Handbook (Version 8), December 2019. https://www.ueq-online.org/Material/Handbook.pdf, as of June 9, 2022.

[36] Martin Schrepp, Jörg Thomaschewski, and Andreas Hinderks. Construction of a Benchmark for the User Experience Questionnaire (UEQ). *Journal of Interactive Multimedia and Artificial Intelligence*, 4(4):40–44, 2017.

[37] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *ACM Conference on Computer and Communications Security*, pages 161–172. ACM, 2013.

[38] Verena Zimmermann and Nina Gerber. The Password Is Dead, Long Live the Password – A Laboratory Study on User Perceptions of Authentication Schemes. *International Journal of Human-Computer Studies*, 133(1):26–44, 2020.

Appendix

A Interview Questions

General Perception of Windows Hello

- You've been using Windows Hello for the past four weeks, how happy are you with it?
- Can you explain the differences between *password/smartcard* login and Windows Hello?
- Did you encounter any problems logging on to the PC over the past four weeks?
  - How have you solved them?

Use of Biometrics

Skip these questions if participant doesn't have biometric hardware available.

- Your device has a *facial recognition camera/finger print reader*, have you used this/these feature(s)?
  - How often have you used *facial recognition/finger print recognition* compared to the *PIN*?
- What stopped you from using *facial recognition/finger print recognition*?
- Which login method have you used most and why?

Perceived Authentication Speed

- How much time do you spend per login with Windows Hello compared to *password/smartcard*?

Perceived Security

- Please rate the security of Windows Hello.
  - Do you think there is a difference between *facial recognition*, *finger print recognition*, and *PIN* in terms of security?
  - Are there any security issues you see with the use of Windows Hello?

Satisfaction

- Windows Hello is available on many laptops and desktop computer, would you use it on your personal Windows computer?
- Is there anything you like in particular about Windows Hello?
- Is there anything you dislike about Windows Hello?
- Would you rather continue using Windows Hello or return to the traditional *password/smartcard*?

B Codebook

Table 2: The codebook used to code the interviews.

Code	IDs	Description	Example
General Perception of Windows Hello			
Hello is fast	P1, P2, P3, P4, P5, P6, P7, P8, P10, P13	Windows Hello is seen as a fast way of authentication.	*"The speed, I boot up and can start working right away, wouldn't know what could make it better now."* (P13)
Uses / Considers to use Hello personal devices	P1, P2, P3, P4, P7, P8, P9, P10, P13	Participant considers to use, or already uses, Windows Hello with his personal devices at home.	*"On my private laptop I'm using the fingerprint, that is also convenient."* (P3)
Continue using Hello	<*all*>	Participant wants to continue using Windows Hello after the study.	*"No, no, the number combination was more appealing to me, I wouldn't want to go back to the password now."* (P8)
Hello is convenient	P2, P6, P7, P11, P12, P13	Windows Hello is seen as a convenient way of authentication (compared to the password).	*"It was definitely more convenient than before, I had a longer password before."* (P7)
Hello is easy	P1, P2, P3, P5, P10, P13	Windows Hello is easy to learn and easy to use (compared to the password).	*"It was easier with the PIN. So, I found the handling better than before."* (P3)
Preferred Sign-in Method			
Prefers Face	P13	Participant prefers facial recognition over all other methods.	*"And with facial recognition, it's just a much easier recognition, you know, you are signed-in through then just the facial recognition."* (P13)
Prefers PIN	P7, P8, P9, P10, P11, P12	Participant prefers PIN over all other methods.	*"The number combination. Yes, because as I said, it was a tad faster."* (P12)
Reservation Against Biometrics			
Availability risks	P2, P4, P11	Participant describes risks regarding the availability of the authentication method (e.g. camera is not working, fingerprint is not detected).	*"The fingerprint recognition, I could imagine, if you have wet hands, so that's not the case with us now, but if your hands are wet or have a possible injury, then you would have maybe problems with the sign-in."* (P2)
Accustomed to PIN	P8, P8, P9, P10, P11	Participant is used to use the PIN and prefers it over other methods.	*"Yeah, I'm kind of used to typing."* (P10)
Laptop lid closed	P6, P7, P10	The laptop is docked and the lid is usually closed which covers the biometric sensors of the device and makes them unavailable until the lid is opened manually.	*"I tried it once, but yes, by the fact that I actually always have the laptop closed, that would have been a circumstance for me to use it that way."* (P7)
Laptop too far away	P11, P12	The laptop is docked and on the other side of the desk which brings the biometric sensors out of reach.	*"What is a bit stupid is that the notebook is not frontal to the monitor, if I now had a camera directly on the monitor it would certainly be a bit better."* (P11)
Too secure / unnecessary	P6, P8, P11	Windows Hello is seen as too secure and unnecessary for this type of scenario it is used in.	*Personally, I don't see this as a necessity.* (P11)

Table 2: Continued from previous page

Code	IDs	Description	Example
Fear of being observed	P9, P10, P11, P12	Participant feels observed through the web cam pointing at them.	*"Then I have the feeling that I am am being watched."* (P12)
Perceived Authentication Speed			
Hello is faster	<*all*>	Authentication can occur faster using Windows Hello compared to the password.	*"Yeah, between half and 3/4 as long as the password, around the twist, I'd say."* (P6)
Perceived Usability			
Hello nothing to carry	P5, P12, P13	Participants do not have to carry an additional token/device.	*"You don't always have to carry the stick with you and you can't forget it."* (P12)
Hello fewer errors	P2, P3, P4, P6, P8, P9	Participant faces fewer authentication failures when signing-in (e.g. due to mistyped password).	*"I mistype less, with upper and lower case letters or something, because it was just numbers."* (P4)
Hello memory-wise less effort	P4, P7, P8, P11, P13	Participant needs to remember less information to sign-in, a six-digit PIN is always shorter than a password with minimal length of 10 characters.	*"And I can remember it better, because sometimes, especially after a vacation, you kind of forget the password."* (P4)
Perceived Security			
Biometrics most secure (no difference between face/fingerprint)	P9	Participant considers biometrics as most secure authentication method, fingerprint and facial recognition are seen as equally secure sign-in options.	*"But basically, the two sign-in options seem to be equally secure to me."* (P9)
No difference between Hello methods	P11	Participant considers all sign-in options of Windows Hello as equally secure.	*"Yes, I would put them in the same category."* (P11)
Facial recognition most secure	P1, P2, P3, P4, P8, P10, P12, P13	Participant considers facial recognition as most secure sign-in option.	*"If you now take facial recognition again and also the fingerprint, I also have the impression that facial recognition is easier, better and more secure."* (P13)
Password most secure	P4, P7, P11	Participant considers traditional passwords as most secure sign-in option.	*"So I suppose it's also secure, but yes, in theory it seems more insecure than a long password."* (P7)
Fingerprint most secure	P6	Participant considers fingerprint as most secure sign-in option.	*"Yeah, I think fingerprint is probably even more secure than facial recognition, so purely emotionally, but yeah."* (P6)
PIN most secure	P5	Participant considers PIN as most secure sign-in option.	*"No, I think the PIN is even more secure."* (P5)

C Additional Plots

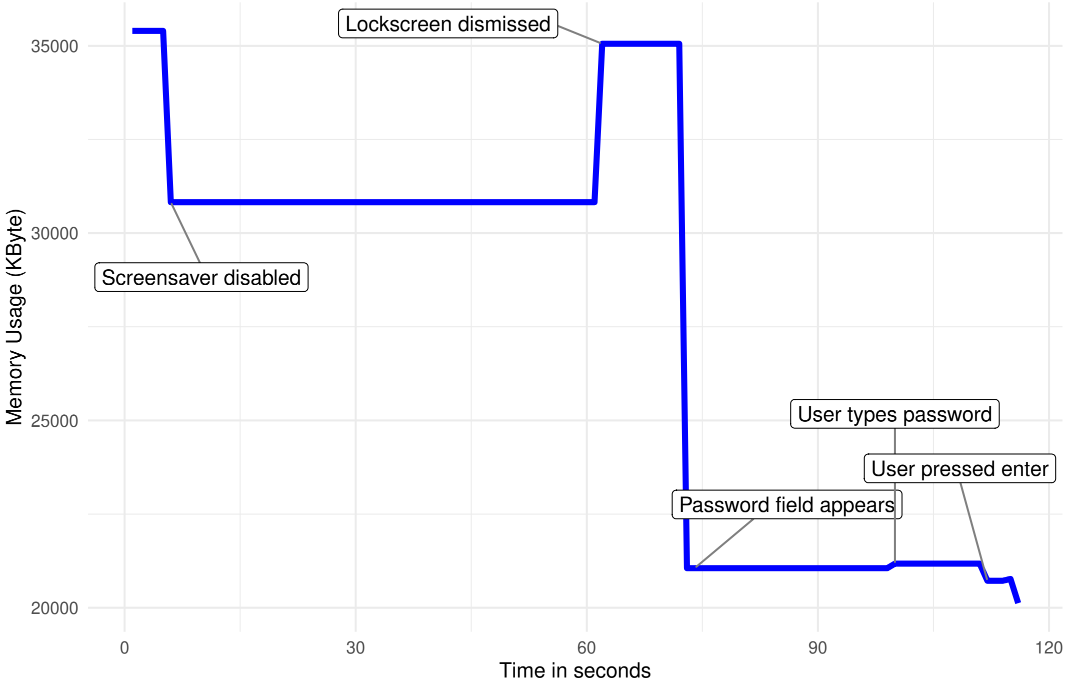


Figure 6: Example of a memory profile of Microsoft's LogonUI used to determine the sign-in timings.

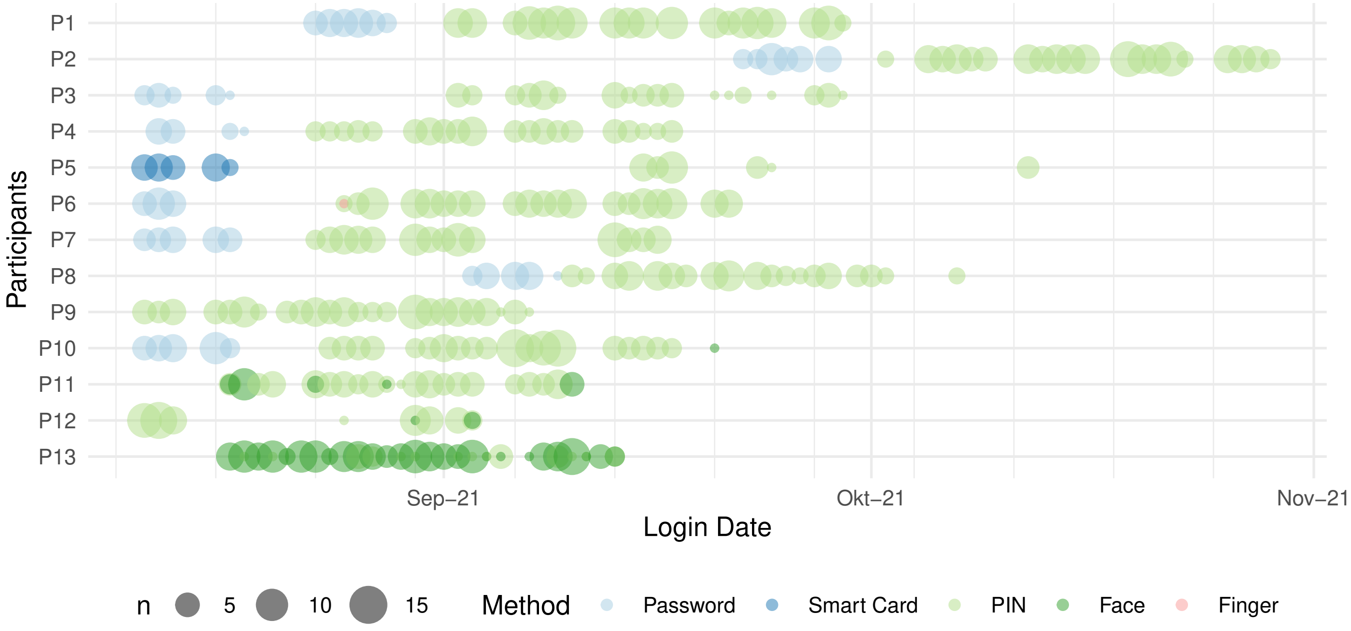


Figure 7: Sign-ins of the participants over the course of the study.