sustainability

MDPI

Article

Reviewing the Usability of Web Authentication Procedures: Comparing the Current Procedures of 20 Websites

Abdulmohsen Saud Albesher

The Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal University, Hofuf 31982, Saudi Arabia; aalbesher@kfu.edu.sa

Abstract: A sustainable online environment is essential to protecting businesses from abuse and data breaches. To protect sustainability, websites' authentication procedures should continuously keep up with new technologies and the ways in which these technologies are used. Thus, a continuous assessment of these authentication procedures is required to ensure their usability. This research aimed to compare the status of the sign-up, sign-in, and password recovery processes on 20 websites. The researcher checked every website in a separate session and used the "think-aloud" technique while recording the screen to ensure accurate data analysis. Specific items were checked during every session to detect the similarities and differences between the tested websites in their authentication processes. The results led to valuable discussions and recommendations for improving authentication procedures. Some of these recommendations include best practices for better design of password rules, determining when two-factor authentication should be compulsory, and understanding how to improve password reset processes and keep accounts secure.

Keywords: security; sustainable security; usability; authentication; websites; review; passwords; sign-up; sign-in; password reset

Citation: Albesher, A.S. Reviewing the Usability of Web Authentication Procedures: Comparing the Current Procedures of 20 Websites. *Sustainability* **2023**, *15*, 11043. https://doi.org/10.3390/su151411043

Academic Editor: Marc A. Rosen

Received: 15 June 2023
Revised: 12 July 2023
Accepted: 13 July 2023
Published: 14 July 2023

1. Introduction

Cybersecurity issues are central to today's technology-driven economy. Cyber security has become a key need in providing a sustainable and secure society for internet users in cyberspace. Protecting users includes applying the most effective authentication procedures. Indeed, authentication procedures are continuously changing because of developments in the technology people use. Designers' understanding of humans and their capabilities has been improving through sciences, such as human–computer interaction. What was the best practice yesterday may be unsuitable today. For instance, 15 years ago, the average user had about 25 accounts that required a password [1]. With the increased usage of the internet, this number has doubled. A recent report showed that, currently, people have an average of 80 accounts requiring passwords [2]. This significant change should lead designers to consider whether a password is still the preferred authentication method because more accounts increase the likelihood of needing to reset passwords. The procedures for resetting passwords differ from one website to another, and the most common procedure is to rely on email or phone numbers. Another method is to use security questions. Users typically select security questions to answer when registering for a new website. One problem with this method is that the answers to these questions may be found on social media [3,4]. Another problem occurs with websites that are not used frequently because it may be hard to remember the answers to the questions after a long period of time. Other procedures include using a user's registered devices, which are the ones they use regularly and have been saved in the service provider's systems.

Although security has a human component that must neither be disregarded nor neglected [5], system engineers and designers are rarely taught how to enhance system features while preserving effective decision-making. Security designers must prioritize

usability while developing the web authentication process because it only becomes a priority when users complain. Indeed, users disregard or work around ineffective security products [6]. Users tend to only care about security once their accounts are hacked [7].

Most studies focus on alternatives to current security procedures because statistics show evidence of increased data breaches and security hacking. The number of data breaches in the United States has increased by 170% over the past 10 years, from only 662 in 2010 to over 1800 in 2021 [8]. Some studies have focused on one security procedure, such as resetting passwords [9–11]. Other studies have focused on only one part of a security procedure, such as password policies [12–17] or password meters [18–22]. Some research has focused on specific authentication methods, such as passwords [23–25], biometrics [26–29], or two-factor authentication [30–35]. Some have discussed the particular issues of one authentication method, such as the difficulty of remembering many passwords [36–38], while others have examined solutions to this issue, such as password managers [39–41]. However, many of these studies have focused on usability from the technical side rather than from the human side. To the best of our knowledge, only one series of studies has evaluated various aspects of authentication procedures and discussed their usability and security issues [42–45]. There are more issues to be tested that require a larger sample. Existing authentication procedures must be studied, beginning with registration procedures, continuing through login procedures, and ending with account recovery procedures.

Some scholars have highlighted the importance of studying the usability of authentication procedures [46,47]. Braz et al. [48] describe the need for usable security principles in the authentication process. This research contributes to the literature by providing some recommendations that help improve the usable security of web authentication methods. To write these recommendations, the current authentication procedures were evaluated and compared with the current state of the sign-up, sign-in, and password reset processes on 20 websites. The researcher checked every website in a separate session and used the "think-aloud" technique while recording the screen to ensure accurate data analysis. During every session, the researcher checked specific items to uncover the similarities and differences between the tested websites in their authentication processes. The anticipated results of the present study could assist designers in developing stronger security procedures that consider human capacities, thereby making procedures easier to utilize and improving the user experience.

The current paper is structured as follows: The first section of this research is divided into a three-part introduction. In the first and second parts, the terms "sustainable security" and "usable security" are defined. Passwords, password policies (rules), and password meters are discussed in the third part because they are essential in website authentication procedures. The present paper's second section discusses related work, and the third section describes the methodology. The remaining sections are the results, discussion, recommendations, and conclusions.

1.1. Sustainable Security

Sustainability is not limited to environmental issues [49]. In the cyber domain, security entails the prevention of unauthorized access, while sustainability can be defined as maintaining continuous services for users [50]. Some researchers [51] have looked at sustainable security as realigning security objectives to meet users' needs. A sustainable and secure society for internet users is an essential demand in cyberspace because it maintains the security of data and information. Sustainable cybersecurity must be implemented to safeguard any firm from fraud and data breaches [52]. Sustainable security is influenced by factors such as confidentiality, integrity, availability, and energy consumption [51]. Sustainability factors must be incorporated into security procedures from the very beginning of development [53].

Some researchers have indicated three nodal areas of software sustainability: human, economic, and environmental sustainability [54]. When designing authentication procedures, the human factors must be considered; otherwise, the relationship between users and

service providers would be unsustainable. Although the security of the services relies on machines for authentication processes, human intervention can create cyber sustainability problems. For example, there are password regulations that touch practically everyone. A rigid, onerous reset procedure that places too much of a burden on users—whether consumers or employees—quickly costs money and is difficult to maintain. For example, consider a business user who twice tries to log into their account but is unsuccessful; as a result, the system automatically locks the business owner out. The user must then call the help desk and wait for a representative to become available before having the account reset. This is an inefficient and unsustainable process that burns through time, energy, and attention.

1.2. Usable Security

The International Organization for Standardization (ISO) 9241-11 [55] defines usability as "the extent to which a system, product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" ([56] para. 2). The ISO/International Electrotechnical Commission (IEC) 27,000 is an international standard for information security and defines information security as the "preservation of the confidentiality, integrity, and availability of information" (as indicated in [57], p. 5). Merging the concepts of security and usability in information technology means allowing users to complete a task effectively, efficiently, and satisfactorily without any errors that may cause security threats. In the present study, we define usable security procedures as those created to be human capable and that can ensure a high level of protection from cyberattacks. There is always a trade-off between security and usability. The more secure a system is, the less usable it is and vice versa [58]. Usability is a vital part of any system's development [59].

Human users are the most important part of the security procedures for any software products, systems, or services because they create and use passwords, which are the first line of defense against attacks. Users must meet security rules when creating passwords. However, there is often little concern shown for human factors in the design of security procedures [51], which may lead users to become frustrated with the wasted time and effort in understanding these procedures. In the worst-case scenario, the users may leave the system if they can. To better deal with these issues, experts have attempted to utilize their knowledge of usability and security together. Whitten and Tygar [60] indicate that a security system is usable when its users understand security tasks and how to complete them without errors. The interface should also encourage users to reuse the system [51].

There are different types of methods that apply the principles of usability and security together. One type is inspection methods, which are based on one expert or a group of experts who can evaluate a user interface and critique its compliance with specific guidelines for usability and security [61,62]. This type of method aims to identify security vulnerabilities and usability issues. Another type is the experimental method, which involves participants. Ismailova [63] has tested the usability and security of government websites in the Kyrgyz Republic, finding various errors. Naiakshina et al. [64] experiment with the security of users' registration on social networking from the developers' perspective by recruiting student developers.

1.3. Passwords

Passwords are a critical component of any authentication process. Alphanumeric passwords are popular for several reasons, one being that developers can quickly implement them at a low cost on websites, applications, or other software [65]. Another reason for their popularity is their reliability because they are thoughts in users' minds that are hard to steal. However, there are a number of effective methods for attackers to guess passwords, and they are often hard to memorize [66]. Users must follow best practices to secure their passwords [67]. Although various scholars have predicted that passwords will die, they have continued to be the best available choice for authentication [68]. Indeed, new

techniques, such as two-factor authentication, have given passwords more reliability and longevity [69].

1.3.1. Password Policies

Password policies are the requirements or rules shown to users when they are creating their passwords. Services ask users to follow policies to ensure that they create strong passwords [68]. In most cases, users are only able to complete their registration if they meet these requirements. Password policies vary from one service to another. Some standard policies include eight characters that must include at least one uppercase letter, one lowercase letter, and one special character. Other policies may include prohibiting dictionary words or commonly used words such as "admin." The differences in password policies lead users to face problems with generating and remembering passwords, as indicated in [70]. To overcome these problems, users can apply different strategies. One strategy is to use personal information, such as a birthday or location, as part of the generated password [71]. This strategy leads to passwords that may look complex but can still be guessed [72]. Another strategy is repeating the same password but for different accounts [73]. This may increase the chance of multiple accounts being hacked when a hacker obtains the password file of reused passwords [74]. The problem is that systems cannot detect whether users have reused their passwords, so this behavior continues [68].

1.3.2. Password Meters

Password meters or password checkers help users meet password policies or create strong passwords by giving them real-time feedback about the strength of their newly generated passwords [75]. These meters use different words and colors to describe the level of secure passwords. For instance, some meters use three colors to describe a password's security level: red for weak, orange for fair, and green for strong. Some meters explain the problems with the newly generated passwords and how to fix them [76]. Other meters show password composition rules in a list, and every time the user meets one of them, the color of the listed rule changes, or the meter shows a green tick mark beside it, which helps users detect the problem. Password meters use heuristics to guide users toward good passwords. Some heuristics predict what users will type [77]. Other heuristics compare a user's password to other users' passwords to show how strong the newly generated password is [78,79].

2. Related Work

Bhana and Flowerday [80] encouraged using a particular type of passphrase by finding that user-friendly passphrases are better than traditional passwords for user authentication. Sahin and Li [81] empirically studied the impact of typo-tolerant password authentication using password leak datasets. Jang and Kim [82] tested whether customers' interactions with an online service could be affected by the culture and usability of the online security service. Kawu et al. [83] studied the relationship between culture and password behavior to determine whether this affects password strength. Rasmussen [84] looked at the usability of roaming software tokens and whether they could replace passwords. Simmons et al. [85] examined the usability of 12 password managers by evaluating specific use cases and design paradigms. Jeong and Jung [86] proposed a password manager that creates a master password that consistently works with other passwords on a user's devices without storing any passwords. Kariryaa and Schöning [75] presented a new approach to the password meter. When users create a new password, the system looks at their personal information on social media. If their personal information is used in the password, the system suggests that the newly created passwords are weak and can be guessed from public information.

Seitz et al. [13] conducted an online experiment to determine whether users would create stronger passwords when provided with a decoy tool. The decoy tool tests users' passwords and suggests stronger passwords in a colorful way. The results were mixed, and there were no significant effects of the decoy tool found. Seitz et al. [87] argued

for the need for different password policies to avoid password reuse. They indicated that websites should have different password policies to force users to create different passwords for different websites. They presented a new approach that minimizes the number of passwords reused by studying the top 100 websites in Germany, as ranked on Alexa.com. The results showed the possibility of maintaining password strategies that could work for 83 of 100 websites. Seitz [88] believed that password policies should be different for all users. Thus, this study proposes a new approach that provides changeable policies depending on users' personal information. The author recommends using this approach because passwords tend to survive for a long time. Verkijika [89] evaluated password practices for 37 e-commerce websites in South Africa and reported poor practices for around 92% of the tested websites. Maoneke and Flowerday [15] studied the password policies of the top 30 websites in South Africa in terms of the number of visits. Tsokkis and Stavrou [72] attempted to improve password creation strategies to help users build strong passwords. They proposed a new tool that educates users on how to avoid weak passwords generated by mixing symbols with personal information.

3. Methodology

Inspection methods can help identify the usability issues of such a system and provide helpful recommendations to improve its usability [90]. One of the inspection-based methods, called the "individual expert review", has been selected to evaluate the usability of web authentication procedures. During the evaluation, the expert discovers usability flaws based on the rules of thumb and his experience [91]. Thus, the evaluator does not have to follow a specific template during the analysis to capture usability flaws and provide some recommendations. This approach has been used in one series of studies [42–45] that measures the usable security of websites.

In the individual expert review, a single expert looks at specific data about a service while playing the part of a user to identify systemic flaws using a variety of techniques, including an individual walkthrough, a review of the service against specific heuristics, or testing various perspectives of the service. [92] This method has been used by several research papers that have purposes similar to those of the current research [60,93,94]. Some reasons for selecting this method are that no usability labs, participants, or significant expenditures are required [86]. However, the key reason is the ability to test a wide range of websites. For example, only a few websites can be tested with experiments that include participants.

The researcher reviewed and compared the processes of signing up, signing in, and recovering passwords on 20 websites. This sample should be large enough because other studies [42–45] that have applied the same method for a similar purpose have used fewer websites. Moreover, the present study is more compressive because it compared a variety of items for three different authentication processes. During the sign-up process, the researcher noted information related to the primary key for registration (email or phone number), accepting external accounts, hiding the password while typing, retyping the password, password rules, password meters, robot checks, and verification. During the sign-in process, the reviewer collected information related to the types of sign-in options, such as the "stay signed in" feature, hiding the password while typing, and procedures after login failure, such as robot checks and locking accounts. During the recovery process, the researcher collected information about the type of recovery method used, password rules, whether they were changed, retyping the password, robot checks, and adding an alternative primary key.

To diversify the sample, the researcher reviewed security procedures for 20 websites in five domains (reservation, social media, shopping, entertainment, and tech services). The reason for this diversity is that the responses taken by websites in one domain may not be suitable for other domains. For instance, some social media sites partially freeze accounts when there is suspicious login activity. However, they still allow the user to log in but with limited activities. This practice might not be appropriate for websites in other

domains, such as the reservation domain. Thus, besides presenting a comparison with all websites in all domains, the present research explored the opportunity to examine the practices of websites in the same domain. The tested websites were selected based on their popularity according to Statista.com and Similarweb.com. Some websites were skipped because they were the same domain or because they were prohibited in some countries because of their sexual content. The researcher also avoided using more than one website from the same company because the password procedures could be the same. The final selection included Hotels.com, Booking.com, Airbnb, and Marriott Bonvoy for reservation; Facebook, Snapchat, TikTok, and Twitter for social media; Alibaba, Amazon, eBay, and Rakuten for shopping; Dailymotion, IMDb, Netflix, and Spotify for entertainment; and Google, Apple, HUAWEI, and Microsoft for tech services.

The researcher used a new email on Yahoo and a new cell phone number for the purpose of the study. Yahoo was selected because it was not one of the tested websites. QuickTime player was used to record every session. The researcher ensured that the microphone was on for the "think-aloud" technique. This technique requires that "the subject keeps on talking, speaks out loud whatever thoughts come to mind while performing the task at hand" [95]. This technique helped the researcher have a recorded voice for all the usability issues that were captured while examining the website. Thus, this technique allowed for more accurate data analysis. Think-aloud enables evaluators to express their opinions while evaluating a system, which aids in learning more about how the system is used beyond simple behavior tracking. The think-aloud technique is one of the most frequent techniques for evaluating usability [96]. The benefits of using this technique include that evaluators may quickly implement the "think-aloud" method, capture intrinsic cognitive processes that cannot be seen, comprehend the causes of problems with ease, and manage immediate reactions to system operations [97].

The researcher took a screenshot of any new notes, such as the expression used by the website to evaluate the entered password or that guided the user in creating a good password. The experiments were conducted in May 2021. The video for each experiment was watched separately several times, and then, the data were written up as notes in a Word document. After completing this procedure for all websites, the researcher compared the 20 websites to find similarities and differences between their password practices. A table was created to summarize standard information, and additional information was added for explanation and discussion. The videos were watched repeatedly, and the data were written up in the text as notes Figure 1 summarizes the steps involved in the study design.

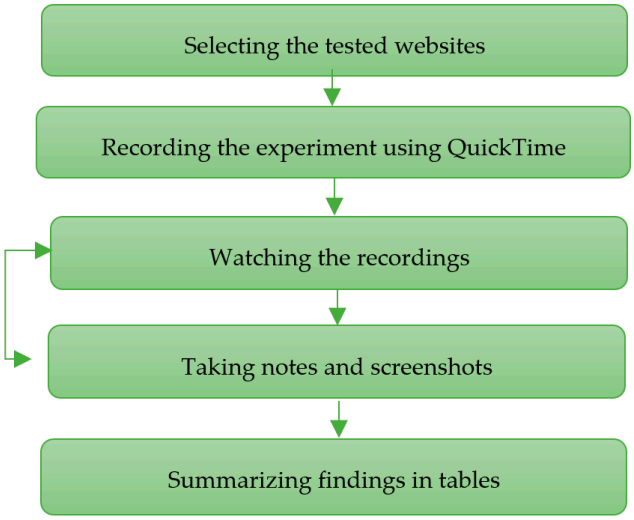

Figure 1. The steps involved in the study design.

4. Results

4.1. Sign-Up Process

The results of the sign-up process showed that 11/20 websites allowed users to sign up using their Google, Facebook, or other accounts (See Appendix A Table A1 for details). Additionally, 11/20 of websites allowed the viewing of passwords while typing, commonly presented with the word "show" or with an icon that looked like an eye. A total of 15/20 websites asked users to follow specific rules when creating new passwords, as shown in Table 1. Some websites had additional rules that remained unknown unless the entered password violated them. For instance, some websites did not accept repeating numbers. The rules of Facebook, Netflix, and Microsoft appeared after clicking the button to sign up or move to the next step, while Snapchat's rules appeared after the user began typing. The minimum required characters were commonly 6 or 8. However, Booking.com asked for ten, and Netflix asked for a minimum of four characters. Some websites called special characters punctuation marks or symbols, while Bonvoy named them just "characters".

Table 1. Password rules for each tested website.

Website	Password Rules
Hotels	6–20 characters, with at least one number
Booking	Minimum 10 characters, including uppercase letters, lowercase letters, and numbers
Airbnb	Cannot contain the name or email address of the account holder, requires at least eight characters and a number or symbol
Bonvoy	8–20 characters (lowercase letters, uppercase letters, numbers, or characters)
Facebook	No rule until clicking sign-up button; at least 6 characters (letters + numbers + punctuation marks)
Snapchat	No rule until the user starts typing; at least eight characters; (may use a) mix of uppercase letters, lowercase letters, numbers, and or/symbols
TikTok	8–20 characters (letters, numbers, and special characters)
Twitter	Eight characters or more
Alibaba	6–20 characters—must contain at least two of each (letters, numbers, and symbols)
Amazon	At least six characters
eBay	At least six characters, containing a number or symbols
Rakuten	eight characters or more
Dailymotion	Minimum eight characters (at least one letter, at least one number, and at least one symbol)
IMDb	At least eight characters
Netflix	No rule until clicking "continue"; 4–60 characters
Spotify	Unknown
Google	Eight or more characters with a mix of letters, numbers, and symbols
Apple	Eight or more characters; uppercase and lowercase letters, at least one number
HUAWEI	At least eight characters
Microsoft	No rule until clicking "next"; at least eight characters; at least two each of uppercase letters, lowercase letters, numbers, and symbols

A total of 15/20 websites provided immediate feedback (meter) for the newly generated password (see Table 2). Five websites (Facebook, Amazon, IMDb, HUAWEI, and Microsoft) did not provide a meter. On some websites, the meter worked while the user typed. On other websites, the meter worked only after attempting to move to the following field or clicking the button for the next step. Five websites (Airbnb, Bonvoy, TikTok, Alibaba, and Dailymotion) showed every rule in a different line, and their colors changed when they were met. However, Airbnb's meter generated inaccurate results. Some websites used red

when rules were not satisfied, while others used gray. The remaining results of the sign-up process showed that 13/20 websites asked for the password to be retyped, 7/20 websites had robot tests, and 13 verified the primary key/s for the account holder (email and/or phone number).

Table 2. Summary of the meter for each tested website.

Website	Immediate Feedback (Meter)
Hotels.com	Worked after moving to the next field (the field turned red when there was a mistake, and a message in red under the field showed the mistake)
Booking.com	Worked after clicking "Create account"; a message in red showed the unsatisfied rules one by one, and the field was in red
Airbnb	Every password rule was on a different line, shown in gray and with an ×; when satisfied, it changed to green and √; password strength was shown (weak = red; good or strong = green)
Bonvoy	Similar to Airbnb, but using red and green
Snapchat	Worked while typing (the word password was in red when moved to its field, and a message in red showed the unsatisfied rule)
TikTok	Worked while typing (every password rule was on a different line and shown in gray color and with an ×; when satisfied, it turned to green)
Twitter	Showed the message "Please enter stronger password" (no specific guidance) in red, and field was in red
Alibaba	Every password rule was on a different line and shown in gray, but with x sign in red; when password rule was satisfied, sign became green √
eBay	A message in gray under the password field; red when the password was simple
Rakuten	Messages "too short", "weak", and "very weak" in red, "fair" in orange, and "strong" and "very strong" in blue
Dailymotion	Similar to Alibaba
Netflix	Worked after clicking "continue" for the first time; red for the message and field
Spotify	Worked while typing; showed a vague message ("too short")
Google	Worked after clicking "next"; both the password field and the message were red
Apple	Similar to TikTok; a line for strength (red, orange = "moderate", green = "strong"); showed password tips
No meter for Facebook, Amazon, IMDb, HUAWEI, or Microsoft	

4.2. Sign-In Process

The results of the sign-in process showed that only 2/20 of websites asked users to retype primary keys (email, phone, username, or ID) after each failed attempt, 13/20 asked users to reenter their password after every failed attempt, 7/20 websites allowed users to view passwords while typing, and 8/20 presented robot tests (See Appendix B Table A2 for details). Some websites showed a robot test only after several failed attempts. A total of 9/20 websites provided the option "stay signed in". The default value for four websites was "no", while the rest were "yes". After failed attempts, 8/20 websites followed the procedure of locking accounts; six websites showed robot tests; two websites asked for a code sent through email; and one website (Facebook) limited the activities of the tested account. Two websites showed the lock time (5 or 30 min), while this remained unknown on other websites.

4.3. Recovery Process

All the tested websites allowed the recovery method to use the registered email or phone number, and some websites provided the opportunity to select an additional recovery method. For example, Google and Apple used registered devices, while Netflix used credit card numbers with first and last names. Bonvoy asked for the member's ID with first and last names, country name, and the zip code for specific countries. Amazon,

eBay, and IMDb offered to call the user as another recovery method. Table 3 shows some comments about specific websites. For example, the Booking, Airbnb, and Bonvoy websites asked users for phone numbers during registration but did not use them as a method for password recovery. Some websites were more flexible with the password created during the sign-up process, since they had fewer password rules, as previously mentioned. However, some of these websites changed their requirements after the first recovery. For example, Amazon provided tips to create stronger passwords, while HUAWEI added more rules and provided a meter.

Table 3. Comments on the recovery process for some websites.

Website	Recovery Process Comments
Booking	The phone number was not used in the recovery process.
Airbnb	The phone number was verified, but it was not used for recovery.
Bonvoy	The phone number was not used for password reset.
Facebook	Users could skip creating a new password.
Amazon	Password rules remained the same, but there were some tips.
eBay	User was not asked to change their password.
Rakuten	Only American phone numbers could be added.
Google	Phone and alternative emails were re-added during registration.
HUAWEI	More password rules were added with a meter.
Microsoft	User had to answer security questions after the code.

5. Discussion

The results showed that there are still many differences between websites in terms of security procedures. These differences can confuse users and place large cognitive demands on their memories. Why do websites differ in security procedures? It is still questionable whether the designers of the security procedures follow any usability standards. Although the present research has included leading websites in different domains, the domain itself was not the reason for the differences in security procedures. More investigations are needed to determine the factors behind these differences. The following sections discuss the findings in different sections based on the tested item.

5.1. Using Other Accounts for Sign-Up

This study shows that 11/20 websites offered users the option of signing up using other accounts, such as Google or Facebook. This feature reduces users' cognitive load by reducing the number of passwords they need to memorize and removing the need to follow new password policies [68,98,99]. However, if the other account has technical issues, the user may not be able to log in to either account. Thus, all users who signed up to Booking.com using their Facebook accounts could not use their accounts on Booking.com when Facebook, WhatsApp, and Instagram were down for around 16 h on Monday, 4 October 2021 [100].

5.2. Masked and Unmasked Passwords

Our results showed that 11/20 websites allowed users to show or hide their passwords while typing. When the password is hidden and formatted in asterisks and the user cannot view it, this is called a masked password. When the user can see a password, it is called an unmasked password [101]. Many usability experts have discussed the harmful effects of masked passwords, such as typing errors and the probability of needing more time to type the password successfully. However, security experts have highlighted the importance of masked passwords in saving users from shoulder surfing. Pidel and Neuhaus [102] conducted an exploratory study to detect the differences between masked and unmasked

passwords when using smartphones. They examined specific metrics, such as typing speed, error rate, and the number of backspaces. They found no significant differences between the two cases. This finding supports the need to enhance security more than usability and could answer why nine websites in our sample provided only the option of masked passwords.

5.3. Retyping Passwords

Our results showed that most websites (13/20) asked users to retype their passwords, which means that more time is required for registration. Retyping passwords helps users avoid typing errors and, therefore, minimizes the number of reset times required. However, Bhana and Floweday [80] concluded that the time required for retyping passwords is not worth it. This requirement has positive usability and security effects on retyping passphrases but not passwords. A similar trade-off between security and usability occurs with the "stay signed in" feature. Our results indicate that almost half of the tested websites (9/20) provided this feature. This feature becomes risky when users have opted in and must uncheck the box to opt out. Some users may not notice this while logging in from public devices. Websites face a similar trade-off with the practices used when the user keeps failing to log in. One practice includes asking the user to repeat their username and password after every failed attempt (2/20), repeat only the password (13/20), or adjust the last entered password (5/20). Another practice is having a robot test after every failed attempt or a certain number of failed attempts. TikTok and HUAWEI included a robot test after the first failed attempt; eBay included a robot test after the third attempt; Airbnb included a robot test after the fifth attempt; Hotels.com included a robot test after the tenth attempt; and Google included a robot test after the thirtieth attempt. The other websites had no robot tests at all. Another practice is locking the user's account or limiting their activities, and our results showed that 8/20 websites locked users' accounts and 1/20 limited user activities. More than half (11/20) did not use this practice.

5.4. Password Rules

Our study showed that password rules varied from one website to another. This variation makes it difficult for users to remember the passwords they have created. This process becomes even more complicated for websites with additional password rules appearing only after password creation. For example, some websites refused to use the last password or repeated numbers, such as "1122". Lee et al. [12] conducted an experimental study on 120 of the most popular websites to examine whether they prevented the use of certain passwords. Their sample included websites that prevented passwords that had been leaked in breaches and those that were easy to guess. Their findings showed that 49/120 websites prevented users from using specific passwords. Thus, users had two options: to repeat their passwords in a way that met the rules of most websites or to accept the challenge of remembering many different passwords. Taking the first option (repeating passwords) means that, if there is a breach in one website, the other accounts of the user would be at risk. In other words, users' bank accounts could be hacked because they used the same passwords for websites or apps with no sensitive data but less security. Stobert and Biddle [103] found that 25/26 of the participants they interviewed reused their passwords. Moreover, Pearman et al. [104] found that 85.07% of passwords created by 154 participants were reused on financial websites, and 95.50% of these passwords were reused on websites in other domains.

Scholars have discussed the abilities of human memory and how difficult it is to remember many passwords [105]. Some experts have indicated that increasing memory load increases the chance of forgetting more items [106]. Remembering many different passwords is incompatible with human capabilities [107]. Thus, some users find a solution to this issue by relying on a password manager (i.e., one password for all). Alkaldi and Renaud [108] indicated that the password manager removes the need to remember password management strategies. However, all passwords become insecure if the password

manager's security is breached [89]. The Saudi government has recognized the issues of passwords and developed a better way to deal with authentication. They have one unified password that can be used for most government services. Recently, they introduced the "NAFATH" app [109], which takes the fingerprints and faceprints of Saudi citizens and residents at the time of first use and saves them for later authentication. When trying to log in to any government services, users must enter their ID without a password. However, users select the correct number that appears to them on the website they are logging into and the app.

5.5. Password Meter

Our study showed that websites used different presentations for meters. Additionally, meters work differently, either post-entry or dynamically, as shown in Table 2. A similar variation in the results was found in another study. Fujita et al. [110] tested 231 websites based on two UX guidelines (friendly timing and friendly explanation). They found that only 35% of the tested websites satisfied these criteria. Moreover, our study found that the Airbnb meter needed to be more accurate. Golla and Dürmuth [111] found no considerable improvement between the accuracy of their tested meters and those available after 2013. They indicated that the accuracy of the actual meters was less than what was proposed in the research. However, the question that should be asked is whether the meter helps users build solid passwords or makes this process complicated or confusing. Several research papers have shown no reliable positive effects on password strength [69]. However, one online study with more than 2000 participants showed that passwords composed with the help of password meters were more secure and harder to guess than those that did not use password meters [112]. Dupuis and Khan [113] proposed a new visualization for meters based on peer feedback. Instead of the traditional progress bar, their meter showed the user how strong their password was by comparing it to other users' passwords. They indicated that this would help users generate stronger passwords than the traditional meter. Zimmermann et al. [19] noted that findings related to the effectiveness of password meters differed from one study to another. Thus, they introduced a hybrid nudge that contained a combination of password feedback, feedback nudges, and additional guidance. This study showed promising results for password strength. Hartwig and Reuter [114] designed nudging that guides users toward better security decisions in password creation, using white-box-based multidimensional visualizations. This design was based on a changeable radar chart. Their findings presented a somewhat effective nudge for short-term efficacy.

5.6. Recovery Process

Regarding the recovery process, it is surprising that the current study showed that only one website relied on security questions (Microsoft). The question here is whether security questions have become ineffective or whether other methods, such as a one-time password (OTP) via text messages or roaming software tokens, are more effective and secure. Bonneau et al. [115] found that users needed help to recall the answers to their selected questions because they had answered them untruthfully. Albesher and Alhussain [3] found that some answers could be found easily on social media. Doerfler et al. [116] compared the usability of different recovery methods, such as knowledge-based and device-based methods. The knowledge-based category tested users' ability to recall pre-registered email, pre-registered phone, last login location, and security questions. They found that security questions were the most challenging method for users, since they skipped them three times more than the other knowledge-based challenges. Moreover, the success rate of security questions was much lower (78%) than that of OTP via text messages (98%).

There are different cases in which the user can only receive an OTP via text messages, such as when traveling, by activating their international messages. Other cases when the OTP cannot be received either by text messages or roaming software tokens can occur if there is no network coverage, the phone is stolen or damaged, or it has no battery [26]. Thus, providing users with more than one option for recovery is highly recommended.

Google provides users with various methods, such as verifying through registered devices, OTP through alternative email, or OTP via text messages. This increases usability and gives users more flexibility, which facilitates the recovery process. However, it is important to check with users often whether they still have these methods or need to update them. The previously discussed cases for OTP become more annoying for users when OTP is used along with the password for sign-in.

6. Recommendations

There is always a trade-off between security and usability in authentication practices. Specifically, websites that have users' sensitive information always prioritize security over usability. E-commerce or social media websites concerned with engaging more users tend to consider usability more than security. The answers to which best practices should be applied are specific to each individual case.

- Forcing users to abide by specific password rules may help attackers guess a password. Thus, the researcher observed that large companies, such as Google, do not ask users to satisfy specific requirements for newly generated passwords. The researcher believes that this could make the task of guessing more complicated.
- When developers insist on enforcing many password rules, they should all be explicitly shown to users. Developers should not have implicit rules that are discovered only when users break them. This practice wastes users' time. Implicit rules, such as prohibiting the repetition of the same number, should be shown as tips or "other rules".
- Two-factor or multi-factor authentication should be mandatory for websites that have sensitive user information, such as those of banks or hospitals. This two-factor or multi-factor authentication should be optional for other websites to enhance usability.
- Regarding two-factor authentication, users should be granted an alternative option for login when the second factor is unavailable.
- Users should be aware of any login from unrecognized (not registered devices) via email, containing information about the login, such as the type of the device, the location of the login, and the I.P.
- Developers should be required to grant more than one method for password recovery.
- Developers should ask users to perform a security checkup periodically. This checkup should include removing outdated devices, checking recent security events, and updating recovery methods if needed.
- Developers should harness the power of mobile devices that can use the features of biometrics as a method of authentication.
- When using the "stay signed in" feature, developers should treat this feature as opted out, unless the user opts in this feature.

7. Limitations and Future Work

This research was designed to compare the security procedures of 20 websites and discuss their usability based on prior knowledge and experiments. However, empirical research that includes participants is highly necessary. Thus, our future research will evaluate and compare the usability of specific security procedures for different websites in one domain, based on participants' performance and perceptions. Selecting only one domain should provide a fairer and more reasonable comparison. Furthermore, the security procedures of not only websites but also apps need to be evaluated for two reasons. The first is that they have become more useful for completing various tasks in our daily lives. The second is that their security procedures could be different from websites, since mobile devices allow security designers to rely on biometrics for the authentication process.

8. Conclusions

This study evaluated and discussed different procedures for signing up, signing in, and recovering passwords. There is always a trade-off between security and usability

for all the procedures discussed. However, procedures should prioritize security and usability based on the sensitivity of the website's information. There are some noteworthy findings in this research. One is that security questions are no longer the preferred method of password recovery. With the increase in the diversity and availability of tablets and smartphones which offer validation through biometrics, alternative methods could replace passwords in the future. Another noteworthy finding is that some websites have password rules that need to be explicitly described and that are only discovered when users break them. Ultimately, developers should provide more than one option for login and password recovery to give users more flexibility, especially when there are potential obstacles to using the only option provided. Another remarkable finding is that the programming of password meters is complicated and its results may not be accurate which may confuse users. It is better to have no password meters rather than to have a meter with low accuracy.

This study contributes to the knowledge of usable security. It helps the designers of the security procedures to apply the most usable practices by viewing the results of comparing the practices of 20 leading websites and discussing their usability. This study is unique, since it is comprehensive in terms of covering all the web authentication procedures in all three processes: signing up, signing in, and password resetting. It compared the authentication procedures for websites from the same domain and from other domains, since some practices could be suitable only for websites from the same domain but not appropriate for other domains.

Funding: This research is funded by the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia (Project number INST197).

Data Availability Statement: Not applicable.

Acknowledgments: The author extends his appreciation to the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia for funding this research work (Project number INST197). Moreover, the author would like to express special thanks to Amna Asif for her valuable comments.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A

Table A1. Details of the sign-up process.

Category	Website	Primary Key	Accept Other Accounts	Pass Eye	Pass Rules	Pass Meter	Pass Retype	Robot Check	Verification
Reservation	Hotels	Email	√	×	√	√	×	×	×
	Booking	Email	√	√	√	×	√	×	×
	Airbnb	Email/#	√	√	√	√	×	×	×
	Bonvoy	Email	√	×	√	√	√	×	×
Social Media	Facebook	Email/#	×	×	×	×	×	×	√
	Snapchat	#	×	√	×	√	×	×	√
	TikTok	Email/#	√	√	√	√	×	√	√
	Twitter	Email/#	×	√	√	√	×	×	√
Shopping	Alibaba	Email	×	×	√	√	√	×	√ both
	Amazon	Email	×	×	√	×	√	×	√
	eBay	Email	√	√	√	√	×	×	×
	Rakuten	Email	√	√	√	√	×	√	×
Entertainment	Dailymotion	Email	√	√	√	√	×	√	√
	IMDb	Email	√	×	√	×	√	×	√
	Netflix	Email	√	×	×	√	×	×	×
	Spotify	Email	√	×	×	√	×	√	Retype

Table A1. *Cont.*

Category	Website	Primary Key	Accept Other Accounts	Pass Eye	Pass Rules	Pass Meter	Pass Retype	Robot Check	Verification
Tech. Comp.	Google	New email	×	√	√	×	√	×	N.A.
	Apple	Email	×	×	√	√	√	√	√ both
	HUAWEI	Email/#	×	√	√	×	×	√	Email = √ # = optl
	Microsoft	Email/ New email/#	×	√	×	×	×	√	N.A.

means cell phone number. √; × means yes or no.

Appendix B

Table A2. Details of the sign-in process.

Website	Sign-in Options	Email Every Time	Pass Every Time	Pass Eye	Robot Check	Stay Signed In	Account Lock	Comments
Hotels	Email	√	√	×	√	Default = ×	×	Robot after 10 failed attempts
Booking	Email	×	×	√	×	×	√	Locked after 15 fails
Airbnb	Email/#	×	×	√	√	×	×	Robot after five fails (not every time), unless user enters the correct pass
Bonvoy	Email/ Member ID	√	√	×	×	Default = ×	×	N.A.
Facebook	Email/ Member ID	×	√	√	×	×	√	Lock for a few mins after 20 fails + Limit user activities
Snapchat	Email/ Username	×	√	×	×	×	× *	Register using only phone, but sign-in using different options
TikTok	Email/#	×	√	×	√	×	√	Robot after first fail/Shows how many attempts left/Lock for 30 min
Twitter	#/Email/ Username	×	√	×	×	×	×	N.A.
Alibaba	Email/#	×	√	×	×	Default = √	×	A few failed attempts > refresh the page to enter the email again
Amazon	Email/#	×	√	×	×	×	×	After five attempts > takes user to the option of receiving code through email
eBay	Email	×	√	×	√	Default = √	×	Robot after three failed attempts
Rakuten	Email	×	×	×	√	×	×	Robot with every attempt
Dailymotion	Email	×	×	√	×	×	×	N.A.
IMDb	Email	×	√	×	√	Default = √	×	After three fails > robot check every time No lock, but user directed to email code
Netflix	Email	×/√	√	√	×	Default = √	√	Email entered after 20 failed attempts Lock for a few mins
Spotify	Email	×	×	×	×	Default = √	√	Not clear when it is locked
Google	Email	×	√	√	√	×	×	Robot after 30 failed attempts
Apple	Email	×	√	×	×	Default = ×	√	After 10 attempts > locked
HUAWEI	Email/ User ID	×	√	√	√	×	√	Robot after first failed attempt Showed number of remaining attempts after every five fails > lock for 5 min
Microsoft	Email	×	√	×	×	Default = ×	√	After 10 fails > locked

* # means cell phone number. √; × means yes or no.

References

1. Florencio, D.; Herley, C. A large-scale study of web password habits. In Proceedings of the 16th International Conference on World Wide Web, Banff, AB, Canada, 12–14 May 2007.
2. Abdrabou, Y.; Schütte, J.; Shams, A.; Pfeuffer, K.; Buschek, D.; Khamis, M.; Alt, F. "Your Eyes Tell You Have Used This Password Before": Identifying Password Reuse from Gaze and Keystroke Dynamics. In Proceedings of the CHI Conference on Human Factors in Computing Systems, New Orleans, LA, USA, 29 April–5 May 2022.
3. Albesher, A.S.; Alhussain, T. Privacy and security issues in social networks: An evaluation of Facebook. In Proceedings of the 2013 International Conference on Information Systems and Design of Communication, Lisbon, Portugal, 11–12 July 2013.
4. Albesher, A.S.; Alhussain, T. Evaluating and Comparing the Usability of Privacy in WhatsApp, Twitter, and Snapchat. *IJACSA* **2021**, *12*, 251–259. [CrossRef]
5. Atzeni, A.; Faily, S.; Galloni, R. Usable security. In *Encyclopedia of Information Science and Technology*, 4th ed.; Mehdi Khosrow-Pour, D.B.A., Ed.; IGI Global: Hershey, PA, USA, 2018; pp. 5004–5013. [CrossRef]
6. Caputo, D.D.; Pfleeger, S.L.; Sasse, M.A.; Ammann, P.; Offutt, J.; Deng, L. Barriers to usable security? Three organizational case studies. *IEEE Secur. Priv.* **2016**, *14*, 22–32. [CrossRef]
7. Egelman, S.; King, J.; Miller, R.C.; Ragouzis, N.; Shehan, E. Security user studies: Methodologies and best practices. In Proceedings of the CHI'07 extended abstracts on Human factors in computing systems, San Jose, CA, USA, 28 April–3 May 2007.
8. Aslam, M.; Khan Abbasi, M.A.; Khalid, T.; Shan, R.u.; Ullah, S.; Ahmad, T.; Saeed, S.; Alabbad, D.A.; Ahmad, R. Getting Smarter about Smart Cities: Improving Data Security and Privacy through Compliance. *Sensors* **2022**, *22*, 9338. [CrossRef]
9. Huh, J.H.; Kim, H.; Rayala, S.S.; Bobba, R.B.; Beznosov, K. I'm too busy to reset my LinkedIn password: On the effectiveness of password reset emails. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017.
10. Routh, C.; DeCrescenzo, B.; Roy, S. Attacks and vulnerability analysis of e-mail as a password reset point. In Proceedings of the 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 24–25 February 2018.
11. Karim, N.A.; Shukur, Z.; AL-banna, A.M. UIPA: User authentication method based on user interface preferences for account recovery process. *J. Inf. Secur. Appl.* **2020**, *52*, 102466. [CrossRef]
12. Lee, K.; Sjöberg, S.; Narayanan, A. Password policies of most top websites fail to follow best practices. In Proceedings of the Eighteenth Symposium on Usable Privacy and Security, Boston, MA, USA, 8–9 August 2022.
13. Seitz, T.; Hartmann, M.; Pfab, J.; Souque, S. Do differences in password policies prevent password reuse? In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017.
14. Gerlitz, E.; Häring, M.; Smith, M. Please do not use!? or your License Plate Number: Analyzing Password Policies in German Companies. In Proceedings of the Seventeenth Symposium on Usable Privacy and Security, Virtual, 9–10 August 2021.
15. Maoneke, P.B.; Flowerday, S. Password policies adopted by South African organizations: Influential factors and weaknesses. In Proceedings of the International Information Security Conference, New York, NY, USA, 25 January 2019; Springer: Cham, Switzerland, 2019.
16. Al-Slais, Y.; El-Medany, W.M. User-centric adaptive password policies to combat password fatigue. *Int. Arab. J. Inf. Technol.* **2022**, *19*, 55–62. [CrossRef]
17. Grilo, M.; Campos, J.; Ferreira, J.F.; Almeida, J.B.; Mendes, A. Verified password generation from password composition policies. In Proceedings of the International Conference on Integrated Formal Methods, Lugano, Switzerland, 1 June 2022; Springer: Cham, Switzerland.
18. Sreesailam, V.B.; Pentakota, D.G.; Pappala, T.; Kopanati, S.; Siripurapu, C.P. A Novel Methodology Proposed To Produce A Secure Password. *J. Pharm. Negat. Results* **2022**, *13*, 5142–5150. [CrossRef]
19. Zimmermann, V.; Marky, K.; Renaud, K. Hybrid password meters for more secure passwords—A comprehensive study of password meters including nudges and password information. *Behav. Inf. Technol.* **2022**, *42*, 700–743. [CrossRef]
20. Stainbrook, M.; Caporusso, N. Comparative evaluation of security and convenience trade-offs in password generation aiding systems. In Proceedings of the International Conference on Applied Human Factors and Ergonomics, Washington, DC, USA, 6 June 2019; Springer: Cham, Switzerland, 2019.
21. Abdrabou, Y.; Abdelrahman, Y.; Khamis, M.; Alt, F. Think Harder! Investigating the Effect of Password Strength on Cognitive Load during Password Creation. In Proceedings of the CHI Conference on Human Factors in Computing Systems Extended Abstracts, Yokohama, Japan, 18–13 May 2021.
22. Bojato, J.; Donado, D.; Jimeno, M.; Moreno, G.; Villanueva-Polanco, R. Password Guessability as a Service (PGaaS). *Appl. Sci.* **2022**, *12*, 1562. [CrossRef]
23. Jiang, J.; Zhou, A.; Liu, L.; Zhang, L. OMECDN: A Password-Generation Model Based on an Ordered Markov Enumerator and Critic Discriminant Network. *Appl. Sci.* **2022**, *12*, 12379. [CrossRef]
24. Lee, K.; Yim, K. Cybersecurity Threats Based on Machine Learning-Based Offensive Technique for Password Authentication. *Appl. Sci.* **2020**, *10*, 1286. [CrossRef]
25. Hong, K.H.; Lee, B.M. A Deep Learning-Based Password Security Evaluation Model. *Appl. Sci.* **2022**, *12*, 2404. [CrossRef]
26. Baig, A.F.; Eskeland, S. Security, Privacy, and Usability in Continuous Authentication: A Survey. *Sensors* **2021**, *21*, 5967. [CrossRef] [PubMed]

27. Oogami, W.; Gomi, H.; Yamaguchi, S.; Yamanaka, S.; Higurashi, T. Observation study on usability challenges for fingerprint authentication using WebAuthn-enabled android smartphones. In Proceedings of the USENIX Symposium on Usable Privacy and Security, Boston, MA, USA, 9–11 August 2020.
28. Marasco, E.; Albanese, M.; Patibandla, V.V.R.; Vurity, A.; Sriram, S.S. Biometric multi-factor authentication: On the usability of the FingerPIN scheme. *Secur. Priv.* **2022**, *6*, e261. [CrossRef]
29. Stergiadis, C.; Kostaridou, V.-D.; Veloudis, S.; Kazis, D.; Klados, M.A. A Personalized User Authentication System Based on EEG Signals. *Sensors* **2022**, *22*, 6929. [CrossRef] [PubMed]
30. Reese, K.; Smith, T.; Dutson, J.; Armknecht, J.; Cameron, J.; Seamons, K. A Usability Study of Five {Two-Factor} Authentication Methods. In Proceedings of the Fifteenth Symposium on Usable Privacy and Security, Santa Clara, CA, USA, 12–13 August 2019.
31. İşler, D.; Küpçü, A.; Coskun, A. User perceptions of security and usability of mobile-based single password authentication and two-factor authentication. In Proceedings of the Data Privacy Management, Cryptocurrencies and Blockchain Technology, Luxembourg, 20 September 2019; Springer: Cham, Switzerland, 2019; pp. 99–117.
32. Sun, Y.; Zhu, S.; Zhao, Y.; Sun, P.A. User-Friendly Two-Factor Authentication Method against Real-Time Phishing Attacks. In Proceedings of the 2022 IEEE Conference on Communications and Network Security, Austin, TX, USA, 3–5 October 2022.
33. Peeters, C.; Patton, C.; Munyaka, I.N.; Olszewski, D.; Shrimpton, T.; Traynor, P. SMS OTP Security (SOS) Hardening SMS-Based Two Factor Authentication. In Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, Nagasaki, Japan, 30 May–3 June 2022.
34. Marky, K.; Ragozin, K.; Chernyshov, G.; Matviienko, A.; Schmitz, M.; Mühlhäuser, M.; Eghtebas, C.; Kunze, K. "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Trans. Comput.-Hum. Interact.* **2022**, *29*, 1–32. [CrossRef]
35. Bruzgiene, R.; Jurgilas, K. Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication. *Electronics* **2021**, *10*, 1819. [CrossRef]
36. Yıldırım, M.; Mackie, I. Encouraging users to improve password security and memorability. *Int. J. Inf. Secur.* **2019**, *18*, 741–759. [CrossRef]
37. Woods, N.; Siponen, M. Improving password memorability, while not inconveniencing the user. *Int. J. Hum.-Comput. Stud.* **2019**, *128*, 61–71. [CrossRef]
38. Guo, Y.; Zhang, Z.; Guo, Y. Optiwords: A new password policy for creating memorable and strong passwords. *Comput. Secur.* **2019**, *85*, 423–435. [CrossRef]
39. Alodhyani, F.; Theodorakopoulos, G.; Reinecke, P. Password Managers—It's All about Trust and Transparency. *Future Internet* **2020**, *12*, 189. [CrossRef]
40. Chaudhary, S.; Schafeitel-Tähtinen, T.; Helenius, M.; Berki, E. Usability, security and trust in password managers: A quest for user-centric properties and features. *Comput. Sci. Rev.* **2019**, *33*, 69–90. [CrossRef]
41. Avram, C.; Machado, J.; Aştilean, A. Hardware Passwords Manager Based on Biometric Authentication. *Eng. Proc.* **2021**, *6*, 31. [CrossRef]
42. Furnell, S. An assessment of website password practices. *Comput. Secur.* **2007**, *26*, 445–451. [CrossRef]
43. Furnell, S.; Bär, N. Essential lessons still not learned? Examining the password practices of end-users and service providers. In Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust, Las Vegas, NV, USA, 21–26 July 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 217–225.
44. Furnell, S. Assessing website password practices—Over a decade of progress? *Comput. Fraud Secur.* **2018**, *7*, 6–13. [CrossRef]
45. Furnell, S. Assessing website password practices—Unchanged after fifteen years? *Comput. Secur.* **2022**, *120*, 102790. [CrossRef]
46. Cho, G.; Huh, J.; Kim, S.; Cho, J.; Park, H.; Lee, Y.; Beznosov, K.; Kim, H. On the security and usability implications of providing multiple authentication choices on smartphones: The more, the better? *ACM TOPS* **2020**, *23*, 1–32. [CrossRef]
47. Kruzikova, A.; Knapova, L.; Smahel, D.; Dedkova, L.; Matyas, V. Usable and secure? User perception of four authentication methods for mobile banking. *Comput. Secur.* **2022**, *115*, 102603. [CrossRef]
48. Braz, C.; Seffah, A.; Naqvi, B. *Integrating a Usable Security Protocol into User Authentication Services Design Process*; Auerbach Publications: Boca Raton, FL, USA, 2018.
49. Alismail, M.A.; Albesher, A.S. Evaluating Developer Responses to App Reviews: The Case of Mobile Banking Apps in Saudi Arabia and the United States. *Sustainability* **2023**, *15*, 6701. [CrossRef]
50. Mardani, A.; Jusoh, A.; Zavadskas, E.; Cavallaro, F.; Khalifah, Z. Sustainable and renewable energy: An overview of the application of multiple criteria decision making techniques and approaches. *Sustainability* **2015**, *7*, 13947–13984. [CrossRef]
51. Agrawal, A.; Alenezi, M.; Kumar, R.; Khan, R.A. A Unified Fuzzy-Based Symmetrical Multi-Criteria Decision-Making Method for Evaluating Sustainable-Security of Web Applications. *Symmetry* **2020**, *12*, 448. [CrossRef]
52. Sadik, S.; Ahmed, M.; Sikos, L.F.; Islam, A.K.M.N. Toward a Sustainable Cybersecurity Ecosystem. *Computers* **2020**, *9*, 74. [CrossRef]
53. Venters, C.; Jay, C.; Lau, L.; Griffiths, M.K.; Holmes, V.; Ward, R.; Xu, J. Software sustainability: The modern tower of babel. In Proceedings of the Third International Workshop on Requirements Engineering for Sustainable Systems Co-located with 22nd International Conference on Requirements Engineering (RE 2014), Karlskrona, Sweden, 25 August 2014; Volume 1216, pp. 1–6.
54. Calero, C.; Piattini, M. Puzzling out software sustainability. *Sustain. Comput. Inform. Syst.* **2019**, *16*, 117–124. [CrossRef]

55. *ISO 9241-11:2018*; Ergonomics of Human-System Interaction—Part 11: Usability: Definitions and Concepts. ISO: Geneva, Switzerland, 2018.
56. Nigel, B.; Carter, J.; Earthy, E.; Geis, T.; Harker, S. New ISO standards for usability, usability reports and usability measures. *Lect. Notes Comput. Sci.* **2016**, *9731*, 268–278.
57. von Solms, B.; von Solms, R. Cybersecurity and information security—What goes where? *Inf. Comput. Secur.* **2018**, *26*, 2–9. [CrossRef]
58. Di Nocera, F.; Tempestini, G. Getting Rid of the Usability/Security Trade-Off: A Behavioral Approach. *J. Cybersecur. Priv.* **2022**, *2*, 245–256. [CrossRef]
59. Alhejji, S.; Albesher, A.S.; Wahsheh, H.; Albarrak, A. Evaluating and Comparing the Usability of Mobile Banking Applications in Saudi Arabia. *Information* **2022**, *13*, 559. [CrossRef]
60. Whitten, A.; Tygar, D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium, Washington, DC, USA, 23–26 August 1999.
61. Mathiasen, N.R.; Bødker, S. Threats or threads: From usable security to secure experience? In Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges, Lund, Sweden, 18–22 October 2008.
62. Alharbi, J.A.; Albesher, A.S.; Wahsheh, H.A. An Empirical Analysis of E-Governments' Cookie Interfaces in 50 Countries. *Sustainability* **2023**, *15*, 1231. [CrossRef]
63. Ismailova, R. Web site accessibility, usability and security: A survey of government web sites in Kyrgyz Republic. *Univers. Access Inf. Soc.* **2017**, *16*, 257–264. [CrossRef]
64. Naiakshina, A.; Danilova, A.; Tiefenau, C.; Smith, M. Deception task design in developer password studies: Exploring a student sample. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security, Baltimore, MD, USA, 12–14 August 2018.
65. Watanabe, Y.; Suzuki, H.; Naito, K.; Watanabe, A. Proposal for User Authentication Method Combining Random Number and Password. In Proceedings of the 2019 IEEE 8th Global Conference on Consumer Electronics GCCE, Osaka, Japan, 15–18 October 2019.
66. Guan, A.; Chia-Mei, C. A Novel Verification scheme for Resisting Password Guessing Attacks. In Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing, Aizuwakamatsu, Japan, 30 January–2 February 2021.
67. Breitinger, F.; Tully-Doyle, R.; Hassenfeldt, C. A survey on smartphone user's security choices, awareness and education. *Comput. Secur.* **2020**, *88*, 101647. [CrossRef]
68. Siponen, M.; Puhakainen, P.; Vance, A. Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Comput. Secur.* **2020**, *88*, 101617. [CrossRef]
69. Everett, C. Are passwords finally dying? *Netw. Secur.* **2016**, *2*, 10–14. [CrossRef]
70. Marky, K.; Mayer, P.; Gerber, N.; Zimmermann, V. Assistance in daily password generation tasks. In Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, Singapore, 8–12 October 2018; pp. 786–793.
71. Li, Y.; Haining Wang Kun, S. A study of personal information in human-chosen passwords and its security implications. In Proceedings of the IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–14 April 2016.
72. Tsokkis, P.; Stavrou, E. A password generator tool to increase users' awareness on bad password construction strategies. In Proceedings of the 2018 International Symposium on Networks, Computers and Communications, Rome, Italy, 19–21 June 2018; pp. 1–5.
73. Das, A.; Joseph, J.; Caesar, M.; Borisov, N.; Wang, W. The tangled web of password reuse. In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 23–26 February 2014.
74. Florêncio, D.; Herley, C. Where do security policies come from? In Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, USA, 14–16 July 2010.
75. Kariryaa, A.; Schöning, J. Moiprivacy: Design and evaluation of a personal password meter. In Proceedings of the 9th International Conference on Mobile and Ubiquitous Multimedia, Essen, Germany, 22–25 November 2020.
76. Ur, B.; Alfieri, F.; Aung, M.; Bauer, L.; Christin, N.; Colnago, J.; Cranor, L.F.; Dixon, H.; Emami Naeini, P.; Habib, H.; et al. Design and evaluation of a data-driven password meter. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017.
77. Komanduri, S.; Shay, R.; Cranor, L.; Herley, C.; Schechter, S. Telepathwords: Preventing Weak Passwords by Reading Users' Minds. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 591–606.
78. Agholor, S.; Akinyemi, I. A Peer Pressure Method for Helping End-Users Generate Strong Passwords. *Int. J. Cyber-Secur. Digit.* **2018**, *7*, 480–488.
79. Egelman, S.; Sotirakopoulos, A.; Muslukhov, I.; Beznosov, K.; Herley, C. Does my password go up to eleven? The impact of password meters on password selection. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris, France, 27 April–2 May 2013.
80. Bhana, B.; Flowerday, S. Usability of the login authentication process: Passphrases and passwords. *Inf. Comput. Secur.* **2022**, *30*, 280–305. [CrossRef]
81. Sahin, S.; Li, F. Don't Forget the Stuffing! Revisiting the Security Impact of Typo-Tolerant Password Authentication. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 15–19 November 2021.

82. Jang, J.; Kim, H. Diverging influences of usability in online authentication system: The role of culture (US vs Korea). *Int. J. Bank Mark.* **2022**, *40*, 384–400. [CrossRef]
83. Kawu, A.A.; Orji, R.; Awal, A.; Gana, U. Personality, Culture and Password Behavior: A relationship study. In Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities, Windhoek, Namibia, 3–7 December 2018; pp. 1–4.
84. Rasmussen, B. A Usability Study of FIDO2 Roaming Software Tokens as a Password Replacement. Doctoral Dissertation, Brigham Young University, Provo, UT, USA, 2021.
85. Simmons, J.; Diallo, O.; Oesch, S.; Ruoti, S. Systematization of Password Manager Use Cases and Design Paradigms. In Proceedings of the Annual Computer Security Applications Conference, Virtual Event, 6–10 December 2021.
86. Jeong, H.; Jung, H. Monopass: A password manager without master password authentication. In Proceedings of the 26th International Conference on Intelligent User Interfaces-Companion, College Station, TX, USA, 14–17 April 2021.
87. Seitz, T.; Emanuel von Zezschwitz, E.; Meitner, S.; Hussmann, H. Influencing self-selected passwords through suggestions and the decoy effect. In Proceedings of the 1st European Workshop on Usable Security, Darmstadt, Germany, 18 July 2016.
88. Seitz, T. Personalizing Password Policies and Strength Feedback. In Proceedings of the Second International Workshop on Personalization in Persuasive Technology co-located with the 12th International Conference on Persuasive Technology, PPT@PERSUASIVE 2017, Amsterdam, The Netherlands, 4 April 2017; pp. 64–69.
89. Verkijika, S. An Evaluation of the Password Practices on Leading e-Commerce Websites in South Africa. *Commun. Comput. Inf. Sci.* **2019**, *973*, 104–114.
90. Lee, S.H. Usability testing for developing effective interactive multimedia software: Concepts, dimensions, and procedures. *J. Educ. Technol. Soc.* **1999**, *2*, 2.
91. Nielsen, J. Usability inspection methods. In Proceedings of the CHI '94, Boston, Massachusetts, USA, 24–28 April 1994.
92. Wilson, C. The Individual Expert Review. In *User Interface Inspection Methods: A User-Centered Design Method*, 1st ed.; Elsevier: Waltham, MA, USA, 2014; pp. 34–48.
93. Alshar'em, M.A.R.W.A.N.; Zin, A.M.; Sulaiman, R.; Mokhtar, M.R. Evaluation of The TPM User Authentication Model for Trusted Computers. *JATIT* **2015**, *81*, 298–309.
94. Krumsvik, O.A.; Babic, A.; Mugisha, A. Design Variations for Improved Usability of Mobile Data Capture in Rural Uganda. In Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Prague, Czech Republic, 3–8 June 2018; Springer Nature: Singapore, 2018; pp. 439–443. [CrossRef]
95. Nielsen, J.; Clemmensen, T.; Yssing, C. Getting access to what goes on in people's heads? Reflection on the think-aloud technique. In Proceedings of the Second Nordic Conference on Human-Computer Interaction, Aarhus, Denmark, 2 October 2002; pp. 101–110.
96. Cotton, D.; Gresty, K. Reflecting on the think-aloud method for evaluating e-learning. *Br. J. Educ. Technol.* **2006**, *37*, 45–54. [CrossRef]
97. Someren, M.; Yvonne, F.; Barnard, Y.F.; Sandberg, J. *The Think Aloud Method: A Practical Approach to Modelling Cognitive London*; Academic Press: Cambridge, MA, USA, 1994.
98. Obada-Obieh, B.; Huang, Y.; Beznosov, K. The burden of ending online account sharing. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25–30 April 2020; pp. 1–13.
99. Zimmermann, V.; Gerber, N. The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *Int. J. Hum.-Comput. Stud.* **2020**, *133*, 26–44. [CrossRef]
100. Wakefield, J. What Happened to Facebook, WhatsApp, and Instagram? *BBC News*. 5 October 2021. Available online: https://www.bbc.com/news/technology-58800670 (accessed on 14 December 2022).
101. Gruschka, N.; Iacono, L. Password Visualization beyond Password Masking. In Proceedings of the Eighth International Network Conference, Heidelberg, Germany, 6–8 July 2010; pp. 179–188.
102. Pidel, C.; Neuhaus, S. Breaking: Password entry is fine. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2019; Volume 11594.
103. Stobert, E.; Biddle, R. The Password Life Cycle. *ACM Trans. Priv. Secur.* **2018**, *21*, 13. [CrossRef]
104. Pearman, S.; Thomas, J.; Naeini, P.E.; Habib, H.; Bauer, L.; Christin, N.; Cranor, L.F.; Egelman, S.; Forget, A. Let's go in for a closer look: Obseving passwords in their natural habitat. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017.
105. Vu, K.; Proctor, R.; Bhargav-Spantzel, A.; Tai, B.; Cook, J.; Schultz, E. Improving password security and memorability to protect personal and organizational information. *Int. J. Hum.-Comput. Stud.* **2007**, *65*, 744–757. [CrossRef]
106. Neath, I. *Human Memory: An Introduction to Research, Data, and Theory*; Thomson Brooks/Cole Publishing Co.: Pacific Grove, CA, USA, 1998.
107. Kävrestad, J.; Lennartsson, M.; Birath, M.; Nohlberg, M. Constructing secure and memorable passwords. *Inf. Comput. Secur.* **2020**, *28*, 701–717. [CrossRef]
108. Alkaldi, N.; Renaud, K. MIGRANT: Modeling Smartphone Password Manager Adoption Using Migration Theory. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **2022**, *53*, 63–95. [CrossRef]
109. Saudi National Digital Identity Management. Available online: https://www.iam.gov.sa/about.html (accessed on 14 December 2022).

110. Fujita, M.; Yamanaka, T.; Matsuda, N.; Yoshimura, A.; Kanaoka, A. Do authentication websites adopt friendly password registration error message design? In Proceedings of the SENIX Symposium on Usable Privacy and Security, Boston, MA, USA, 7–9 August 2022; pp. 1–5.
111. Golla, M.; Dürmuth, M. On the accuracy of password strength meters. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1567–1582.
112. Renaud, K.; Zimmermann, V. Nudging folks towards stronger password choices: Providing certainty is the key. *Behav. Public Policy* **2019**, *3*, 228–258. [CrossRef]
113. Dupuis, M.; Khan, F. Effects of peer feedback on password strength. In Proceedings of the 2018 APWG Symposium on Electronic Crime Research, San Diego, CA, USA, 15–17 May 2018; pp. 1–9.
114. Hartwig, K.; Reuter, C. Nudging Users Towards Better Security Decisions in Password Creation Using Whitebox-Based Multidimensional Visualizations. *Behav. Inf. Technol.* **2022**, *41*, 1357–1380. [CrossRef]
115. Bonneau, J.; Bursztein, E.; Caron, I.; Jackson, R.; Williamson, M. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In Proceedings of the 24th International Conference on World Wide Web, Florence, Italy, 18–22 May 2015.
116. Doerfler, P.; Thomas, K.; Marincenko, M.; Ranieri, J.; Jiang, Y.; Moscicki, A.; McCoy, M. Evaluating Login Challenges as A Defense Against Account Takeover. In Proceedings of the World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019.