


Review

Usable Security: A Systematic Literature Review

Francesco Di Nocera ^{*}, Giorgia Tempestini and Matteo Orsini

Department of Planning, Design, and Technology of Architecture, Sapienza University of Rome, 00196 Rome, Italy; giorgia.tempestini@uniroma1.it (G.T.); matteo.orsini@uniroma1.it (M.O.)

* Correspondence: francesco.dinocera@uniroma1.it

Abstract: Usable security involves designing security measures that accommodate users' needs and behaviors. Balancing usability and security poses challenges: the more secure the systems, the less usable they will be. On the contrary, more usable systems will be less secure. Numerous studies have addressed this balance. These studies, spanning psychology and computer science/engineering, contribute diverse perspectives, necessitating a systematic review to understand strategies and findings in this area. This systematic literature review examined articles on usable security from 2005 to 2022. A total of 55 research studies were selected after evaluation. The studies have been broadly categorized into four main clusters, each addressing different aspects: (1) usability of authentication methods, (2) helping security developers improve usability, (3) design strategies for influencing user security behavior, and (4) formal models for usable security evaluation. Based on this review, we report that the field's current state reveals a certain immaturity, with studies tending toward system comparisons rather than establishing robust design guidelines based on a thorough analysis of user behavior. A common theoretical and methodological background is one of the main areas for improvement in this area of research. Moreover, the absence of requirements for Usable security in almost all development contexts greatly discourages implementing good practices since the earlier stages of development.

Keywords: usable security; usability; security; cybersecurity; cyber-security; authentication; developers; guidelines; behavior



Citation: Di Nocera, F.; Tempestini, G.; Orsini, M. Usable Security: A Systematic Literature Review. *Information* **2023**, *14*, 641. <https://doi.org/10.3390/info14120641>

Academic Editors: Moutaz Alazab and Ammar Alazab

Received: 29 September 2023

Revised: 15 November 2023

Accepted: 28 November 2023

Published: 30 November 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Usable security refers to the design and implementation of security measures considering users' needs, abilities, and behaviors. As systems become more secure by implementing authentication mechanisms and encryption protocols, they become more complex and less intuitive for users. This complexity can result in a steeper learning curve, greater effort required to perform tasks, and potential frustration for users. On the other hand, systems prioritizing usability may sacrifice some security measures, making them more susceptible to cyber-attacks [1].

Thus, usable security aims to make security measures more effective by minimizing user errors and increasing user compliance with security protocols.

When the concept of usable security began to spread in the mid-1990s, authors initially focused primarily on the security of passwords and emails. The security of passwords is a good example illustrating the trade-off between usability and security because of the practice of saving login credentials for convenience [2]. It is evident that storing a unique and complex alphanumeric string for each account is expensive for the individual [3] but, on the other hand, saving passwords introduces risks. If a malicious user gains access to the device or account, they would have immediate access to all the stored passwords, compromising multiple accounts simultaneously. To avoid these risks, it is essential to balance usability and security.

From a security perspective, strategies such as using complex and unique passwords or frequently updating them promote security. However, they can lead to user frustration

and the adoption of insecure practices, such as writing passwords on easily accessible surfaces [4].

Subsequent studies, however, have expanded the field of usable security by investigating how to integrate intuitive interfaces, clear instructions, simplified authentication processes, and educational resources into systems that ensure security. The goal is to help users make security decisions that ensure both security and usability without the need for significant cognitive or operational burdens on users.

In recent years, many research groups and agencies have addressed the balance between security and usability, particularly after the increase in Internet use (including smart working and e-commerce) stemming from the COVID-19 pandemic and a related significant increase in cyberattacks [5–10]. Contributions to this area are variegated. Some of them lie in the experimental and social psychology traditions, and some (many) others are established in the computer science/engineering frameworks, to name a few types of studies. Therefore, understanding what strategies are used to study this phenomenon and what results have emerged from empirical studies is a goal to be pursued to bring order to the contributions in the literature.

2. Rationale

Our review is not the first review on usable security. Other scholars attempted to review this field of study in academic journal articles. However, many of these contributions lack a systematic approach (e.g., 5, 7, 8). Accordingly, they do not express the inclusion and exclusion criteria, and the selection of articles is based on the authors' narrative choice.

Despite this, we identified a few systematic reviews on the subject, although they primarily dig into more specific aspects over relatively brief periods [6,11,12].

For instance, Distler et al.'s (2021) work aims to scrutinize the methods employed in security and privacy studies, concentrating on the five most pertinent peer-reviewed conference publication venues—a valid choice, though the inclusion of conference papers in systematic reviews is generally unconventional. The review encompasses studies from 2014 to 2018, a constrained and somewhat arbitrary interval, particularly considering the observed upswing in research, especially in recent years, due to technological advancements. Despite analyzing a substantial number of articles, only 6% made it to the final review.

Lennartson et al. (2021) conducted a literature review encompassing both journal and conference papers (again, not a conventional choice) to identify a comprehensive array of factors influencing usability in a security context, including simplicity, information and support, task completion time, error rates, and error management. Despite exploring seven different databases within the 2015–2020 interval, the number of selected articles does not markedly differ from those considered in our review (70 vs. 55 studies).

Nowkedi et al.'s (2016) systematic literature review addressed the gap between usability and security in software development, emphasizing the need to integrate usability and security design for quality end-user software. However, this review is more sectoral, exclusively incorporating engineering works related to the software development domain and not presenting a broader overview of usability and security.

Considering the limitations observed in prior reviews, we have chosen to address usable security using a systematic literature review according to the following assumptions:

- Restrict to academic journal articles, ensuring heightened quality control.
- Examine a substantial timeframe (namely, from 2005 to 2022).
- Encompass studies from diverse research domains rather than confining the scope solely to engineering and computer science.

Our primary objective is to comprehend the state of the art and identify prevalent research trends that have received recognition through publication in scholarly journals.

3. Research Objectives and Research Questions

The research questions (RQs) guided how the literature review was conducted. Based on these RQs, we searched and selected literature since 2005. The first RQ, which is also the main objective of this review, is “Where does the literature stand concerning Usable Security?” (RQ1). Several studies have dealt with the topic of usable security incorrectly by using the term usability. Thus, a univocal way of considering usable security is lacking. That leads to the need to deepen and systematize the existing literature. For this reason, this first research question is relevant to advancing knowledge concerning this topic.

We then set out to identify the macro-areas in which the topic of usable security is covered to answer the question, “How can the contributions found in the literature be classified?” (RQ2). The literature comprises articles that address many issues, target different audiences, and refer to different contexts. Treating these articles as part of a single macro-area may not be helpful in identifying strategies to tackle related cybersecurity issues, as their essential diversity would not be considered. Identifying the aspects that distinguish the different contexts would lead to implementing more appropriate security strategies that combine usability and security. Again, intending to systematize the literature, this second question stems from the need to distinguish the domains in which usable security could be declined.

Finally, the last research question is: “How can scientific research contribute to improving usable security practices in the future?” (RQ3). Considering the importance of this issue and the emergence of new security-related problems due to the faster development of technologies, it is crucial to identify areas where there can be improvements to keep up with cybersecurity issues.

These research questions were formulated to help analyze and compare scientific results and determine the current state of the art and future research directions.

4. Review Process

The approach of our literature review involves the following steps:

- Phase 1. Identification of potential papers that emerged as a result of a literature search on the IEEE and PsycInfo databases;
- Phase 2. Filtering of articles taking into consideration the established inclusion and exclusion criteria (see Sections 4.2.1 and 4.2.2);
- Phase 3. Detailed review of the articles selected in the previous steps;
- Phase 4. Analysis of the results that emerged during the review and discussion.

4.1. Phase 1: Search Strategy for Identification of Potential Papers

4.1.1. Electronic Databases and Digital Libraries

This first phase involved searching for papers on a PsycInfo (Electronic Database) and IEEE Xplore (Digital Libraries) to identify relevant studies. Both databases were searched on 1 December 2022.

- IEEE Xplore (<https://ieeexplore.ieee.org/> accessed on 1 December 2022) provides Web access to more than five million full-text documents from some of the world’s most cited publications in electrical engineering, computer science, and electronics.
- PsycINFO (<https://psycinfo.apa.org/> accessed on 1 December 2022) is a database of abstracts of scholarly journal articles published in all fields of psychology worldwide since the early 1800s. This database contains bibliographic citations, abstracts, cited references, and descriptive information.

The choice of these two databases is due to the cross-cutting nature of the topic of usable security, which is studied by engineers, computer scientists, and psychologists.

4.1.2. Search Procedure

We identified keywords to collect our initial set of papers. Since our goal was to analyze literature that addresses the topic of usable security, a search query was identified

to select papers that mention security and usability, while also considering cybersecurity, which is often closely related to the concept of usable security. The search string used for IEEE Xplore is as follows: (((“Author Keywords”: usability) OR (“Author Keywords”: usable)) AND (“Author Keywords”: security) OR (“Author Keywords”: cybersecurity) OR (“Author Keywords”: cyber-security)); the search string for PsycInfo is, on the other hand, as follows: (KW usable OR KW usability) AND (KW security OR KW cybersecurity OR KW cyber-security).

All articles published in academic journals, excluding conference proceedings and books, that were published from 2005 to 2022 were included in the search.

The first search yielded 80 articles selected after reading the abstracts (see Section 4.2).

4.2. Phase 2: Study Selection

First, we reviewed the 80 studies that emerged from the first search. From this initial analysis, two articles were eliminated as they were present in both searches.

In the next phase, inclusion and exclusion criteria were identified to assess which articles were truly relevant to our research.

4.2.1. Inclusion Criteria

- All empirical works related to the relationship between Usability and Security were included;
- The papers included in the research had to use the term Usability, understood as “the extent to which a product can be used by specific users to achieve specific goals with effectiveness, efficiency, and satisfaction in a given context of use” (ISO-9241-11:2018);
- Only papers written in English (British and American) were included.

4.2.2. Exclusion Criteria

- Review articles were not considered;
- All papers written in languages other than English were not included;
- Works that, from an initial reading of the Abstracts and keywords, did not investigate the relationship between Usability or Security were eliminated;
- The word Usability considered as feasibility and/or “use” led to the exclusion of articles in which it was used in this way.

In light of the criteria discussed above, we assessed the quality of each study and analyzed the title, abstract, and keywords. There was 1 article that was not included because it was not written in English, while 22 were not included because they did not specifically address the security and usability link. As a result, 23 studies that did not meet the criteria were excluded from the study, reducing the search to 55 studies (Figure 1).

4.3. Phase 3: Detailed Review of the Literature

The article selection process led to a detailed review of 55 empirical articles published in International Journals, excluding all reviews and conceptual articles that did not experimentally address the topic. The articles addressed several recurring themes and could be roughly categorized as dealing with the following:

- Usability of authentication methods;
- Helping security developers improve usability;
- Design strategies for influencing user security behavior;
- Formal models for Usable Security evaluation.

The following section (see Section 4.4) provides an overview of the main aspects that were observed during the research and discusses the different categories.

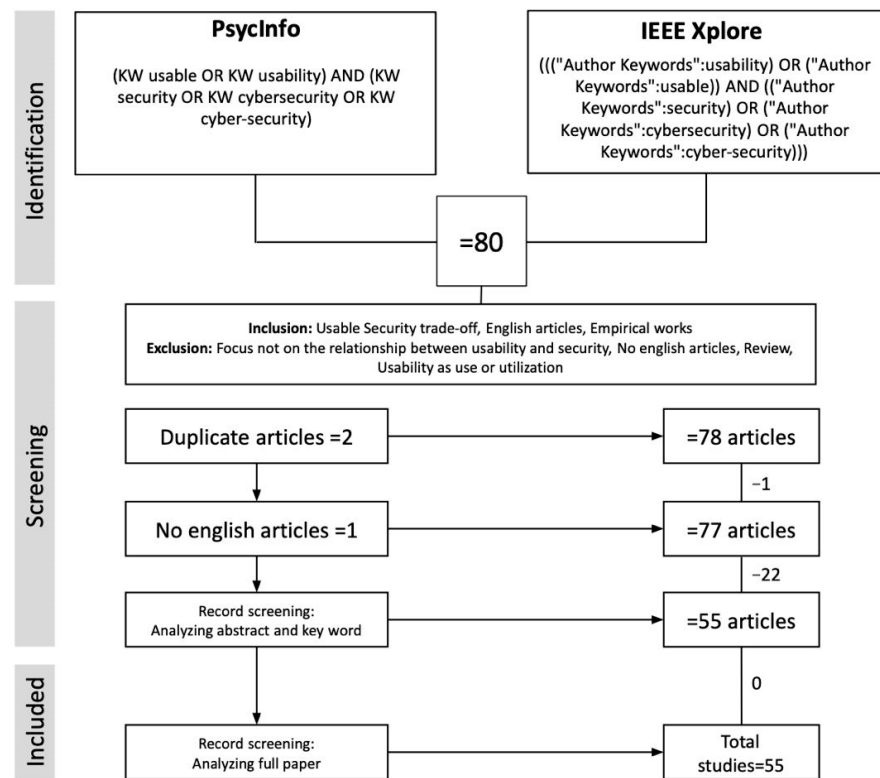


Figure 1. The flow diagram for the review process with the number of included and excluded in each step.

4.4. Phase 4: Analysis and Clustering

Usable Security has attracted growing interest among researchers over the years, as seen from the increasing number of articles published, especially in recent years (Figure 2). The highest number of empirical articles published on the topic has been in the last three years (2020–2022), while a minimal number (only 1 article per year) can be observed from 2005 until 2011). The articles concerning this issue and analyzed in this review were published in several journals, both psychology and computer science/engineering (Table 1). Regarding author affiliation, the United States had the most significant number of articles, followed by the United Kingdom (Figure 3).

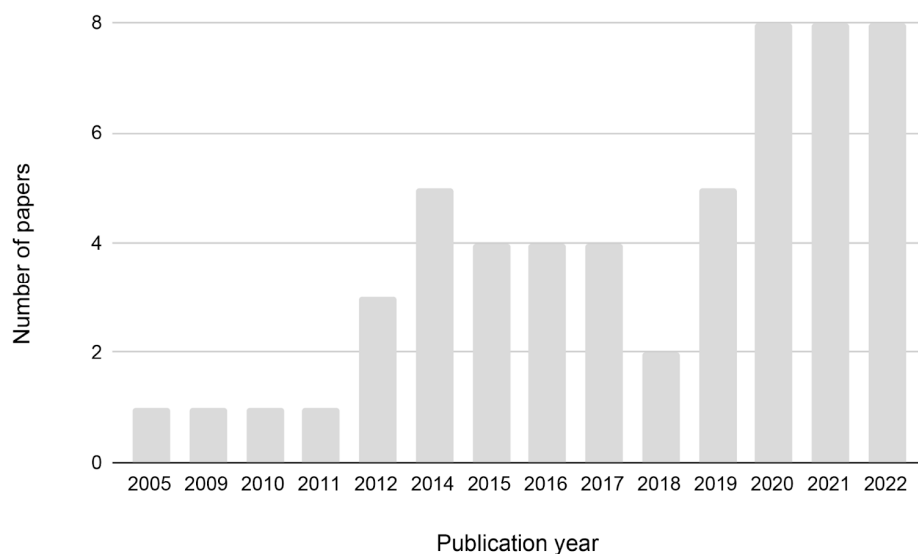


Figure 2. Number of papers from 2005 to 2022.

Table 1. Publication venue and number of articles per journal.

Publication Venue	N. Articles
International Journal of Human-Computer Studies	8
Behaviour & Information Technology	7
IEEE Access	7
IEEE Transactions on Dependable and Secure Computing	6
IEEE Transactions on Information Forensics and Security	3
Interacting with Computers	3
Human Factors	2
IEEE Transactions on Consumer Electronics	2
IEEE Transactions on Mobile Computing	2
Journal of Cognitive Engineering and Decision Making	2
International Journal of Technology and Human Interaction	2
ACM Transactions on Computer-Human Interaction	1
Computers in Human Behavior	1
Frontiers in Psychology	1
IEEE Internet of Things Journal	1
IEEE Transactions on Cybernetics	1
IEEE Transactions on Human-Machine Systems	1
IEEE Transactions on Software Engineering	1
Information & Management	1
Information Systems Research	1
International Journal of Human-Computer Interaction	1
International Journal of Mobile Human Computer Interaction	1

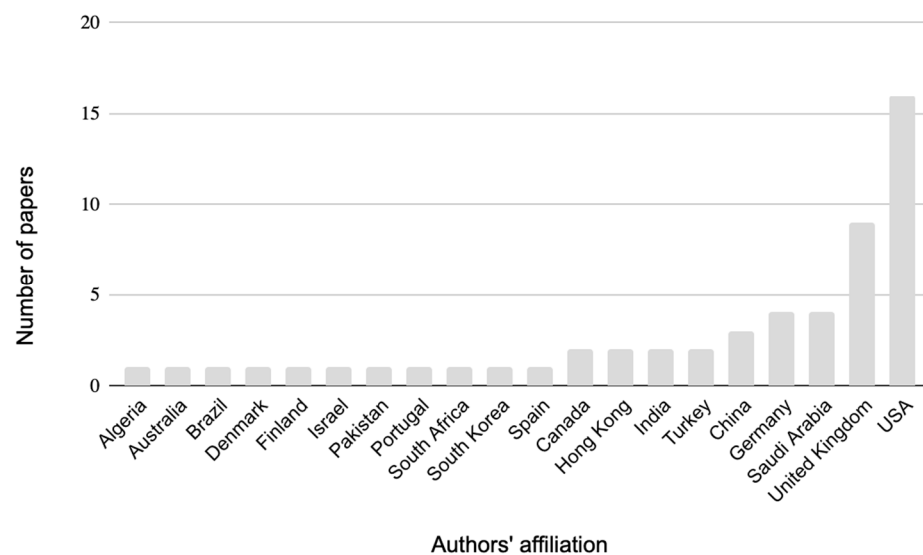


Figure 3. Number of papers published in the country of authors' affiliations.

In the last step of the analysis process, namely full-paper analysis, 55 articles were read, summarized, and discussed. The articles mainly focused on four main research areas: (1) usability of authentication methods, (2) helping security developers improve usability, (3) design strategies for influencing user security behavior, and (4) formal models for usable

security evaluation. The papers mainly focused on authentication, which regarded the largest number of articles (31), while less attention was given to the other topics. The following sections address the identified clusters.

4.4.1. Usability of Authentication Methods (34 Papers)

The articles that fit this theme focus on evaluating the quality of authentication systems, usually focusing on their effectiveness in thwarting cyber-attacks at the expense of a thorough evaluation of their usability. For this reason, the term usable security is misused here because the usability evaluation process occurs after the product is completed, not during the development process. In some of the studies [13], usability is assumed and not even assessed. In addition, only some of the reviewed articles take user satisfaction into account for usability evaluation, focusing almost exclusively on performance. That is a significant shortcoming, as two articles show that performance is often not directly proportional to satisfaction [14,15], although satisfaction is an integral part of usability. Considering the vast number of papers belonging to this cluster (56% of the articles), it has been deemed appropriate to further group them into more detailed sub-clusters.

The sub-clusters were as follows:

- Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA);
- Alternatives to password;
- Virtual environments;
- Proximity-related attacks;
- Usability evaluation of existing and novel systems.

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): One of the tools investigated is CAPTCHA tests [14,16–20]. CAPTCHA is a security measure known as Challenge/Response authentication, aimed at protecting users from spam and password decryption by asking them to pass a simple test that proves the user is a person and not a computer attempting to hack a password-protected account.

However, these studies highlighted the decrease in their effectiveness in distinguishing between humans and machines due to the advancements in machine learning algorithms [19].

The main research objective of these studies is to increase CAPTCHA's security while maintaining acceptable usability for human users. Among the Human Interaction Proofs (HIPs) studied, pure text-based ones were demonstrated as more usable compared to the other methods [14,18]. However, the choice of HIPs should be carefully made depending on the users' attributes, who can perceive HIPs in different ways. Olalere et al., 2014 show that visually impaired users have a higher success rate in solving audio-based CAPTCHAs compared to normal-sighted users. In contrast, text-based CAPTCHAs are demonstrated to be more difficult for foreigners [21].

The most used dependent variables in these studies are performance-related, such as success rate and test resolution time, often leaving out users' satisfaction, which is a relevant element contributing to the usability of a solution.

Alternatives to password: In contexts where traditional text passwords are possible, they are the most preferred method among many [22]. Nevertheless, alternative tools to common text passwords are difficult to use in some contexts and are characterized by vulnerabilities due to the human factor. The predictability of patterns [4] was analyzed, often replacing textual elements with graphical ones [4,15,23–25] and sound-based ones [20].

Some have chosen not to remove textual passwords by creating complex ones in a usable way. Juang and Greenstein [26] allowed users to draw scenes to remind them of senseless phrasal passwords, whereas Biddle et al. [25] allowed users to choose a digital item they owned to generate complex textual passwords.

Others have investigated the use of geographic location as an alternative method of authentication [27,28], which they report to be both usable and secure.

Finally, the concept of using a wearable device to authenticate was explored by Zhang et al. [29] in which the authors integrate existing methods (password, PIN, and fingerprint), proving that this method would increase the security of the authentication methods mentioned above, keeping a (undefined, unmeasured) “high usability”.

Virtual Environments: Some authors have questioned the usability of authentication modes in emerging technological settings, such as virtual reality environments, where the possibilities offered by the three-dimensional environment can determine an increase in security through ways of interaction that could not have been possible before.

Some studies evaluated systems that exploit the third dimension to increase the security of the authentication method while trying to maintain usability [30,31], whereas others focus more on the complex inputs the users give through the advanced wearable systems associated with these environments [30].

Li et al. [32] used login time and login success as indicators of usability. Similarly, Mathis et al. [30] employed login time in their study, involving the manipulation of a cube in different modalities involving touching, moving their eyes, or moving their head. Participants reported feeling more comfortable (usability) when tapping the controller, but using their eyes was preferred in terms of usability and security. Wazir et al. [31] compared their 3D authentication method to an existing one, reporting similar usability and improved security.

Proximity-related attacks: Another central theme is averting attacks based on the proximity of malicious individuals, as in shoulder surfing and eavesdropping. These attacks are possible by gathering visible or audible information from a user nearby. Thus, these solutions focus on using parameters perceivable only by the user [22,23,32,33]. Multimodal schemes have been reported to be promising for secondary authentication, where users feel observed or want to protect sensitive data [33]. Khan et al. [23] evaluated an authentication tool called g-RAT based on a randomized image algorithm using drawings instead of numbers. They reported improved security from shoulder surfing attacks and usability. Al-Ameen and Wright's [27] GeoPass system was found to be not affected by the way a user navigates to the location-password, either by panning on the map or typing the full address in the search bar. Authentication performance (time, attempts) is commonly used to assess usability in all those articles.

Usability evaluation of existing and novel systems: Contributions belonging to this category seem to be characterized by two main approaches to evaluating the products/methods: authors either evaluate them individually [20,25,27,29,34–37] or compare them with other existing or new systems [4,13–19,22,24,26,28,30,32,33,38–41].

In these articles, there is often a misinterpretation of the concept of usability. For example, in many cases, usability is flattened to its efficiency and effectiveness components, evaluating it with parameters such as time to complete tasks and the number of attempts to complete authentication processes [15,16,18–20,24,27,29,33,38]. Sometimes, usability was not evaluated but assumed [32]. Relative to the usability/security trade-off, results are often mixed. For example, some reported how usability decreases as security increases [17], whereas others reported that one changed while the other remained almost unchanged [16].

Several articles lack the information necessary to enable replicability of experiments. For example, Biddle et al. [25] do not report the questions asked of participants.

Another critical issue shared by many articles belonging to this cluster is the creation and use of custom measures to evaluate the usability of the products and systems studied, such as code length [15] or typing effort [39], exclusively related to the specific tool used. This highlights a methodological weakness, forgoing the golden standards for usability assessment and making the studies often not comparable.

In addition, study participants were often college students whose field of study was considered to have little influence in the experiments when, in fact, this parameter would influence their proficiency in computer science. Finally, some studies involved users with special characteristics: users of specific devices [31,36] or with specific characteristics such as visual impairments [18,20] and specific lifestyles [35].

4.4.2. Helping Security Developers Improve Usability (7 Papers)

These articles are aimed at various types of developers, from broader targets such as web/browser/system developers [42,43] to more specific targets such as email system developers [44], junior web developers [45], or even managers and academic developers [46].

The authors tried to find a solution that balances security and usability, guiding developers working in different contexts to ensure a convenient user experience without compromising their data and information protection. In one case, for example, they discuss the importance of including security-related information in the documentation of insecure application programming interfaces (APIs), which, while not explicitly designed for security purposes, if not used properly, can pose risks [45].

Gorski et al. [45] conducted an experiment with 49 junior developers to investigate the following:

1. To what extent does the placement of security-related information in the API documentation influence the transmission of this information to developers;
2. How they read this documentation, focusing on which elements they paid more attention to through the use of eye-tracking;
3. The impact of the presence of cybersecurity instructions (in this case, Content Security Policy—CSP) in the API documentation on the functionality and security of the final product.

The experiment involved completing four programming tasks. The examined developers then sought the solution in the API documentation, but only three groups had it with CSP instructions within it. The remaining control group had the original one provided by Google, lacking cybersecurity-related information.

The experiment demonstrated that the examined developers had “code-oriented” development strategies: they immediately looked for the solution in the functional lines of example code rather than in descriptive parts (departing from a “concept-oriented” approach). This behavioral dynamic did not favor the developers in the control group who, not finding helpful information to solve the problem in the document, resolved it by directly removing the problematic piece of code (related to CSP). On the other hand, it favored those in the group where the API documentation was provided with CSP suggestions in the form of comments in the code that referred to the dedicated chapter. They were better able than the others to solve the problem by making the problematic code part work, thus creating functioning and secure software.

Although developers in the control group created working solutions, none of these were protected by CSP (one candidate even reported, “Let’s just screw security for now”), while most of the solutions developed by candidates in the other groups were protected. The authors argue that the best strategy to draw the developer’s attention to these perceived secondary cross-cutting indications is to place them near the most functional code examples, the first things developers consult with when in difficulty.

They then suggest that library providers provide tailor-made CSP code strings with their service.

In another article, the authors explored the role of GUIs in managing security and privacy settings in social networks [47]. The authors describe a series of security models to assist SNS developers in designing interactive environments that protect individuals’ privacy and security while being extremely user-friendly. Experiments were then conducted to test the proposed models’ effectiveness and compare the models’ GUIs with those currently used on Facebook. The four tasks were structured: Application Request Task, Friendship Request Task, Photo Sharing Task, and Friend List Task. For each task, the following factors were analyzed: user satisfaction, learnability, attitudes, interactivity, and privacy, with participants asked to provide a rating on a Likert scale (from 1 to 5).

The study’s results first showed a strong interest from users in protecting their personal information. Second, it was observed that in all tasks, participants preferred to use the GUIs proposed by the various models rather than those proposed by Facebook, which were more complex and had fewer security-related choice options. The proposed models, therefore,

provide SNS users with appropriate feedback and effective user interfaces that help them make their security and privacy decisions and attempt to strike a balance between usability and security.

Two articles, on the other hand, focus on investigating how to effectively integrate security and usability in the design and implementation of email systems to prevent users from falling victim to phishing attacks [43,44]. Despite sharing the same research area, the studies employed entirely different methodologies. In the study by Alsharnouby et al. [43], participants were shown a series of websites and asked to identify phishing sites. By analyzing eye movements, the authors evaluated participants' success in identifying fraudulent websites, the time they spent observing different screen aspects, and their decision-making rationale. The authors identified various threat types and, for each type, investigated the participants' ability to identify the malicious site: (1) Spoof website with incorrect URL: In general, participants struggled to identify fraudulent banking websites and did not recognize incorrect URLs. However, they successfully identified the Canadian government website that asked them to enroll in identity theft protection. (2) Spoof website with an IP address in URL: only 38% of participants recognized that the Paypal website had an IP address instead of a URL and considered it suspicious. (3) Fake Chrome: Only 62% of participants recognized that a website was a phishing attempt. (4) Popups asking for credentials: 38% of participants were deceived. (5) Overlaid popup windows: 62% of participants recognized the overlaying phishing site, despite a double URL being visible. (6) Fraudulent based on context: 95% of participants successfully recognized the "Credit Card Checker" as a phishing site, likely due to media awareness. (7) Legitimate websites: participants achieved high success rates in recognizing legitimate websites, highlighting their proficiency in identifying what appears "normal" versus what seems suspicious.

In the article by Roth et al. [44], interviews are conducted with 19 users to introduce an innovative design approach for non-intrusive secure email, focusing on the security and usability trade-offs for a specific user group (private non-commercial email users). The approach closely aligns with established engineering principles for designing protection mechanisms, aiming to make the design as simple and small as possible. It avoids complex components like public key infrastructures or the Web of Trust and separates key exchange from binding keys to identities, allowing users to balance usability and security. The design adheres to principles of simplicity, fail-safe defaults, and ease of use. Mail encryption is automatic and transparent, minimizing user interaction. The design provides familiar interaction metaphors and enables users to increase security based on their mail communication statistics, optimizing security utility. The approach aligns with prudent design practices and challenges the need for certification infrastructures for private, non-commercial users. The authors suggest three promising directions for future research: improving human-computer interaction for usable key verification, developing better metrics to maximize security per interaction, and innovative approaches to incentivize security efforts in user interfaces, promoting a foundational level of mail protection.

The work by Flechais and Sasse [42] addresses a more specific issue, attempting to analyze the trade-off problem concerning e-Science. E-Science is a platform that provides many users access to valuable computational resources, data, and software. Insufficient attention to security can lead to cyberattacks that hinder the objective of e-Science, which is to enable the utilization of the resources it offers. The research presented in this article is based on four case studies of e-Science projects. The authors analyzed transcripts and presented a model describing the general factors to consider and the issues identified during security design. Through the use of the ATLAS.ti tool, information was coded, identifying four categories: motivation, responsibility, communication, and stakeholders. As highlighted by the case studies, what emerges is that involving stakeholders in security design provides a highly effective means of identifying their needs. Furthermore, the presence of stakeholders during security design also offers additional benefits in increasing awareness and knowledge of security issues in the system.

Regarding the identified factors, motivation and responsibility are two key aspects that go beyond the scope of a design methodology. The assignment of responsibilities also impacts stakeholders' motivation, remarkably increasing it for those responsible for security. Additionally, the security design process should be engaging, inclusive, and understandable for all participants. Furthermore, one of the key elements of any design exercise is ensuring good communication among participants. Security methods that adopt and support scenarios are much more aligned with how people tend to communicate about security.

The article by Dhillon et al. [46] aims to identify value-based objectives for deciding the balance between security and usability. That approach is very pragmatic, as it seeks to translate abstract concepts into measurable and assessable criteria. After several phases in which objectives were analyzed and reduced through interviews and statistical analysis, the authors identified four final objectives: maximize ease of use and enhance system-related communication, maximize standardization and integration, and maximize system capability. According to the authors, these objectives are helpful for guiding software implementation and development.

The articles above aim to provide insights into how to address this issue, all agreeing that it is necessary to bridge this gap through various strategies, ranging from more technical aspects, such as the precise placement of security information to make it more visible to developers [45], to more general aspects like design simplicity advice to make it more accessible to users.

Analyzing articles in this category has raised significant questions about the methodology employed and the content covered. In particular, the lack of a shared methodology that would enable studies to be replicable and establish a standardized approach to tackle the issue at hand is evident.

The most crucial reflection pertains to the conclusions drawn in these articles: while these articles aim to provide guidance to developers, offering them guidelines on how to address the issue during the design phase, often, the recommendations provided are general and do not seem to be based on genuine empirical work. In some studies, the recommendations resemble reflections on "organizational" aspects, such as (1) the need to assign specific responsibilities to each stakeholder to increase their motivation and prevent the diffusion of responsibilities; (2) understanding the motivations behind the need for security; (3) the security design process should involve, be inclusive, and understandable for all participants; (4) identifying security anecdotes and scenarios [42]. In other studies, the recommendations are very general, focusing on ease of use rather than usability [44], urging developers to concentrate on integrating graphical user interfaces (GUIs) with security aspects to create a user-friendly GUI [43,47]. However, what it means to simplify the design to make GUIs more user-friendly remains unclear. Developers would need more detailed and concrete information on which aspects to consider. Alsharnouby et al. [43] attempt to provide more specific recommendations, such as (1) making the domain more apparent, (2) providing a preview to observe changes, and (3) moving some operations directly to Chrome, even though these aspects are not derived from systematic empirical work.

On the other hand, the study by Gorsky et al. [45] appears to offer more technical recommendations, such as (1) placing cross-cutting instructions near the most functional code examples, which are typically the first things consulted by developers facing difficulties; (2) providing custom CSP code snippets to library providers for their service.

This body of work aims to provide valuable insights into the design of secure systems. However, it also underscores the need for greater methodological rigor and specificity in the recommendations provided to developers.

4.4.3. Design Strategies for Influencing User Security Behavior (10 Papers)

This is by far the most interesting cluster for our goals. Several works within this cluster have addressed the trade-off between usability and security in diverse ways. For instance,

Merdenyan and Petrie [48] attempted to understand whether certain unsafe behaviors related to password usage (such as saving, sharing, and reusing passwords) were driven by underestimating risks or overestimating benefits. In a correlational study conducted with a sample recruited through the MTurk platform, the authors demonstrated that these two dimensions had diverse effects on the likelihood of engaging in specific behaviors. For example, the most crucial component regarding password reuse was the perceived benefit derived from this practice, net of associated risks. That suggests that communication and training interventions should be focused on diversified aspects, depending on the behavior one intends to modify. However, it should be noted that this study did not investigate the actual behaviors enacted by the participants but rather the probability they declared engaging in those behaviors.

Similarly, Haque et al. [49] explored the theme of password reuse, showing that users refer to a hierarchy of password importance based on the type of website. The authors distinguish between “identity” accounts (e.g., email, social networks), “financial” accounts (e.g., online banking), “content” accounts (e.g., personalized services like weather websites), and “sketchy” accounts (e.g., discount and promotion sites). “Financial” sites are attributed higher importance (even greater than “identity” accounts), and therefore, users exercise greater care in creating associated passwords. However, passwords generated for other less important sites often exhibit semantic similarities with those chosen for more critical accounts, making it easier to crack high-value passwords starting from lower-value ones used for sites that presumably implement less efficient protection systems. In an experimental study in which 80 students were asked to generate passwords for various types of sites, the authors could derive up to 20% of high-level passwords from low-level ones using a well-known tool (John The Ripper).

Hirschprung et al. [50] addressed the theme of technology literacy, which refers to the ability to use, manage, understand, and evaluate technology. This skill supports users in deciding how to balance usability and security. For example, knowing the risks associated with saving passwords in the browser might discourage users from employing this procedure (considered advantageous by the user) on specific sites such as those related to online banking. The authors proposed a methodology to optimize the learning process based on specific challenges (short informative videos) demonstrating how hackers can access credit card information saved in the browser. These challenges should provide users with knowledge that can be generalized to other related cases. Although not conclusive, the results of their study (conducted on a sample recruited through the MTurk platform) encourage the adoption of the strategy they proposed because a general level of literacy is not a good predictor of the ability to deal with specific security and privacy threats.

In contrast to previous studies, Steinbart et al. [2] tackled the usability/security trade-off issue by demonstrating that using different input devices (computer keyboard vs. virtual keypad on a smartphone) can modify security behaviors. Since errors can easily occur when using the virtual keypad on a smartphone, adopting precautions to ensure security (such as stronger passwords or passphrases, which simultaneously increase the likelihood of input errors) is hindered. Today, these issues are addressed by biometric authentication methods such as fingerprint or facial recognition. However, using these authentication methods represents a response to the different usability of user interfaces. The study was conducted on a large sample that effectively interacted with a system in both modes, and the authors obtained permission from the Institutional Review Board (IRB) to avoid informed consent that could induce priming effects by providing too much information about the study. This aspect is particularly relevant and raises the issue of disclosing information about experiments in the field of cybersecurity, which often undermines the research effort to comply with human subject experimentation policies. Participants in cybersecurity studies must perceive that information security is genuinely at risk so that the phenomenon can be genuinely investigated.

Other studies within the cluster have investigated the effects of what we could define as “information usability” on security. In particular, a significant problem is identified

in the permissions that apps request from users, which make them less secure, exposing users to sharing information (e.g., location, camera access) often unrelated to the app's functionality. These apps are "over-privileged" and can lead to security and privacy issues. Although users can often choose which permissions to grant, only some have the ability or interest to do so. People often choose apps based on the ratings and trust associated with the app's description.

Gopavaram et al. [51] conducted an experiment using visual information (a numerical value next to the lock icon) and auditory information (cheerful and grave sounds, typical feedback for correct and incorrect responses) to indicate potential privacy risks associated with downloading certain apps. Participants were recruited through the MTurk platform. The results showed that those exposed to this integrated system were likelier to choose apps with higher privacy scores than control groups exposed to a single indicator or no indicators. These findings suggest using specific strategies to direct the user's attention to the permissions required by apps. Unfortunately, the authors do not discuss the different nature of the two indicators. Specifically, the auditory warning is feedback provided immediately after selecting the application (thus, a consequence) and before deciding to install the app. A grave sound (typically associated with an incorrect response) could orient the user's attention to the privacy score (visual indicator) that would otherwise go unnoticed. This interpretation is consistent with the principle of reinforcement in behavior analysis.

Always on the same topic, Gates et al. [52] and Chen et al. [53] suggested that when providing summarized information about the security or risks associated with apps, they should be presented as a "security score" rather than a "risk score". Furthermore, exposure to indicators of app security modifies users' awareness, leading them to actively seek this information even on platforms that do not provide the summarized indicator. These authors have shown that, to improve decision-making, using a positive framing based on security is more effective than a negative framing based on risks. Their studies' results have indicated that user evaluations (often expressed in star ratings) and positive framing influence users' decisions. However, it should be noted that a significant number of subjects in Chen et al.'s (2015) study reported not understanding the security/risk score presented in the form of colored circles, and further analyses conducted by excluding data from these subjects revealed much weaker effects. That raises concerns about experiments conducted through MTurk (a platform widely used in this type of research) and, in particular, the reliability of responses provided by participants.

On the other hand, Wu et al. [54] addressed the issue of the effectiveness of mobile security notifications (MSNs) on mobile devices, which are widely used push notifications to alert users but can also be a source of interruption to the main task, often resulting in being ignored or disabled. In a study that used two types of activities, one "utilitarian" (reading) and the other "hedonic" (playing a game), the authors administered MSNs with varying levels of interruption. In one case, the notification appeared as a pop-up that required the user to take action, interrupting the flow. In contrast, in the other, the notification was a semi-transparent banner that allowed the main task to continue. The results showed that the irritation caused by interrupting the main task did not impact the intention to continue using the app. However, this study used two different interruptions modes in terms of presentation and content: a pop-up indicated high danger, whereas a semi-transparent banner indicated low danger. That introduces a confounding factor of some significance.

Lastly, some works within this cluster have focused on the important topic of electronic payments. For example, Alshamsi and Andras [55] investigated the perceptions of usability and security regarding Bitcoin compared to traditional payment cards, showing that the latter were perceived as more usable and secure. Although the study was not designed to explore the relationship between these two aspects, the authors suggest that the perception of usability influences the perception of security.

The contribution of Zhang and Luximon [56] is more interesting and complex. They compared two systems for electronic payments. The two systems were identical except that one provided feedback on (1) payment status, (2) the identities of the people involved in the transaction, and (3) potential risks during the transaction. In their study, the authors manipulated the presence of the beneficiary (physically present or distant) and the level of trust (known or unknown beneficiary). The results of the study showed that the feedback did not influence the security behaviors of the participants (such as modifying application settings to enhance security and privacy). However, it did influence the perception of security. On the other hand, security behaviors significantly increased under low presence and low trust.

4.4.4. Formal Models for Usable Security Evaluation (4 Papers)

Among the articles we considered, only a handful focused on a particular aspect: the development of usable security models. In one case, Mohamed et al. [57] proposed a meta-model based on existing literature to bridge the gap between a user's and a designer's mental models. The aim was to ensure that the system aligns with the user's expectations of how it should function. However, it is worth noting that this proposed meta-model is quite vague and challenging to implement. Surprisingly, neither the authors nor other research groups have attempted to apply it in subsequent studies.

On the other hand, three other works by Al-Zahrani [58] and Kumar et al. [1,59] ventured into developing estimation methods. These methods aimed to assess the importance of various usability and security attributes by soliciting stakeholders' input. These estimation methods employ fuzzy logic and related techniques, relying on the idea that the chosen solution should strike a balance between being as close as possible to the ideal positive solution and as far as possible from the negative ideal solution. Essentially, these models attempt to establish priorities by ranking and weighting different attributes. However, these frameworks are rather complex and seem somewhat disconnected from the day-to-day practices of designers and developers. In practice, they pose challenges in terms of practical implementation.

5. Discussion

The first goal of this systematic review was to thoroughly examine the existing empirical research on the intricate interplay between usability and security, an interdisciplinary field commonly referred to as "Usable Security" (RQ1). This intersection typically involves a delicate trade-off: increased security measures often result in complexity that hinders usability, whereas user-friendly systems may compromise security integrity. This dynamic presents significant challenges from an organizational perspective.

The contributions reviewed revealed how the complex relationship between usability and security poses significant concerns. Employees often have difficulty complying with complex security protocols and may resort to circumvention when given the opportunity. A careful review of the literature revealed a rich and diverse landscape of studies. The second research question was about classifying these different contributions (RQ2). The studies have been broadly categorized into four main clusters, each addressing different aspects:

1. Usability of authentication methods: These articles aim to evaluate the usability of authentication tools, either by assessing them on their own or by comparing them with similar tools. They have been further divided into sub-clusters: CAPTCHA, alternatives to passwords, virtual environments, and proximity-related attacks.
2. Helping security developers improve usability: The articles in this category concern studies that aim to provide indications to different types of developers to implement the usability of systems without reducing the level of security.
3. Design strategies for influencing user security behavior: The cluster includes studies examining the balance between usability and security in technology usage. The main focus is on individual behavior and the factors influencing the adoption of

secure or insecure behaviors. The studies cover various areas, including password-related behaviors, technology literacy, input device usage, app permissions, security indicators, mobile security notifications, and electronic payment systems.

4. Formal models for usable security evaluation: The cluster includes articles that have attempted to develop usable security models, either devising a meta-model to align user and designer mental models for system consistency or developing estimation methods for usability and security attributes using fuzzy logic and aggregation techniques (Figure 4).

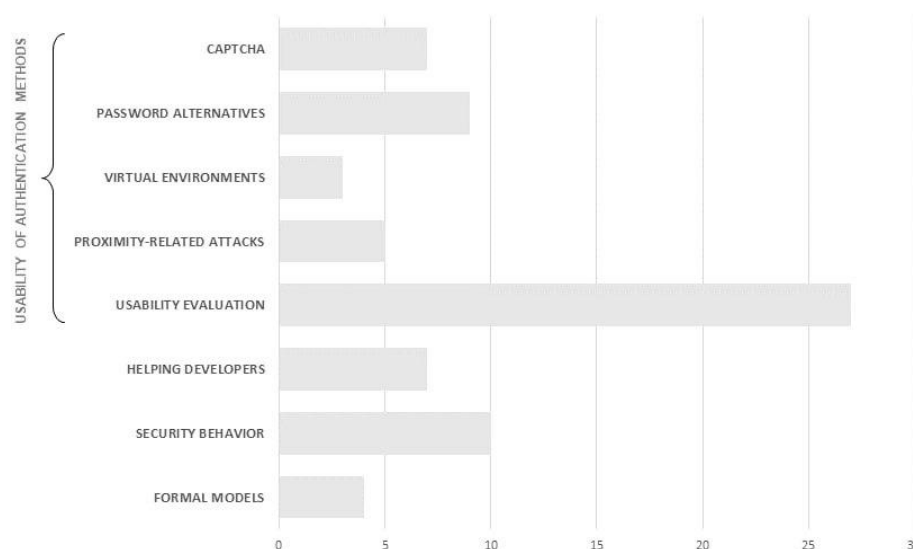


Figure 4. Research objectives of the articles reviewed (please note that some articles may belong to more than one category).

The final research question that this paper investigates is how scientific research can contribute to the future development of usable security (QR3) practices. Studies have shown that there is no standardized way to address this issue, requiring more effort in the future to identify empirically based guidelines that developers and users can adopt. In addition, the work shows how there is a tendency to want to narrow the gap between usability and security rather than explore and exploit it, placing the focus on user behavior.

In contrast, Di Nocera and Tempestini [60] recently attempted to resolve the trade-off issue by proposing to exploit this compromise rather than fighting it. Particularly, in a single-case study in which an individual discriminated between suspicious and non-suspicious emails, they introduced a usability feature as a reinforcer for secure behavior. The results showed increased sensitivity (better performance) during the reinforcement phase compared to the baseline. Of course, this is only an example of how the issue could be addressed. Nevertheless, the lack of a common theoretical and methodological background is one of the main shortcomings of this area of research.

Our review has certain limitations. To begin with, we utilized only two databases, namely IEEE Xplore and PsycInfo. We acknowledge the existence of numerous databases that index articles related to usable security. However, the choice of the number of databases for a systematic literature review is contingent upon the specific focus of the review and the availability of pertinent databases. We opted for PsycInfo and IEEE Xplore due to the interdisciplinary nature of the usable security topic, which attracts contributions from engineers, computer scientists, and psychologists. While including additional databases would decrease the risk of overlooking relevant studies, the selected databases, namely IEEE Xplore (1700 journals) and APA PsycInfo (2319 journals), cover all relevant journals. Moreover, increasing the number of databases searched can lead to the retrieval of more duplicate entries.

In keeping with established practice, we have limited the systematic review to articles published in academic journals. However, this area of study finds a privileged editorial venue in conference proceedings, and thus, our selection may not fully capture the complexity of this area. Consider, for example, the studies by Bravo Lillo et al. [61,62], who examined the habituation effect on the security dialog boxes. This phenomenon reveals that users tend to overlook crucial messages when repeatedly encountering these dialog boxes. Their response often becomes automatic, leading them to press a button to signal their acknowledgment of the warning. Unfortunately, this behavior occurs without understanding the contextual information being presented. These studies have demonstrated how effective security measures require not only notifying users but also a deeper consideration of many aspects (e.g., habits and cognitive processes). Therefore, Bravo Lillo's findings remain relevant for designing security features that genuinely promote and ensure secure user behaviors. Neglecting such contributions may limit the comprehensiveness of any discussion on usable security. On the other hand, a systematic review based on conference contributions has exorbitant numbers and, although many conference papers are peer-reviewed, they offer a different assurance of rigor than articles that have undergone a more thorough selection process.

Also, we only included works that used terms related to usability and security as keywords (i.e., usable, usability, security, cybersecurity, and cyber-security). However, other papers that focus on the study of user behavior concerning security issues may be even more relevant without using the term usability or studying it as such. For example, Hartwig and Reuter [35] have recently compared the effectiveness of two types of password meters (a regular password meter and a radar chart) that provide different levels of detail regarding the robustness of a newly created password. Although they have not framed their research in terms of usable security, their study is based on visual feedback to support decisions in critical situations or signal relevant information (a fairly common strategy in user-centered design). Another recent study, which does not feature the term "security" among its keywords, is the research conducted by Bhana and Flowerday [63]. In their investigation, the authors explored the usability of the login authentication process by conducting a comparative analysis between passwords and passphrases. They introduced passphrases that exclude combinations of lowercase, uppercase, digits, and special characters. Their research explores how passphrases offer enhanced support to users throughout the authentication process, addressing security, memory, and typing issues. We consider contributions like those fully representative of the usable security research field. However, the selection process for that type of article is not straightforward, and the number of articles to be reviewed would quickly rise, making such a selection not practicable in the context of a systematic review. Nevertheless, a narrative review could benefit from greater variety by including relevant contributions that did not find their way here.

6. Conclusions

Based on this literature review, we can state that the term "usable security" is often used loosely. Frequently, it encompasses general usability considerations related to security systems rather than precisely encapsulating strategies aimed at refining the usability of specific security components. As a result, the field's current state reveals a certain immaturity, with studies tending toward system comparisons rather than the establishment of robust design guidelines based on a thorough analysis of user behavior.

In particular, in the context of authentication systems, the notion of usability often revolves around metrics of effectiveness and efficiency and the exclusion of critical aspects such as user satisfaction—a paramount factor in real-world scenarios. It is also worth noting that many of these studies rely on samples from platforms such as Amazon Mechanical Turk (mTurk). While these platforms provide accessibility, the tasks assigned are often divorced from the authentic challenges individuals face in their work environments.

As a final note, a significant portion of the articles focused on developers, and we believe that this specific research activity is strategic to a research agenda on usable security.

Those involved in software design and development greatly influence the implementation of security and, consequently, whether security is implemented in a usable way. In this regard, Gutfleish et al. [64], in a series of 25 interviews conducted in different development contexts, investigated how usable security is handled within the software development process: a process that involves several stages (e.g., requirements definition, code writing, and debugging) and different stakeholders (managers, designers, developers, and customers). The results of that qualitative study showed that the topic of usable security had received little attention within the developer community. That is because usability is often considered to be of lesser importance than security and because it is believed that usability-related aspects do not require specialized knowledge or expertise, but that common sense suffices. As one interviewee reported, “These are things that everyone has to learn on their own to some extent”. Usability is considered entirely independent and less important than security. Indeed, some of the interviewees suggested sacrificing one to achieve the other. Disinterest in usability emerges even more clearly in circumstances where, even in the face of the availability of specialists, the development team chose not to consult with them because consulting with experts was considered a waste of time.

On the other hand, the problem lies in the absence of requirements for usable security in almost all development contexts. Therefore, this aspect is not addressed from the earliest discussions with clients and stakeholders. Likewise, without specific requirements, the need to subject security features to usability assessments is missed. Currently, there are no tools, special documentation, guidelines, or standards for usable security, and this is quite puzzling considering that one of the main objectives of the usable security research field is to inform standardization bodies.

Author Contributions: F.D.N. conducted the literature search; F.D.N., G.T. and M.O. analyzed the abstracts and full papers, wrote the initial draft, and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kumar, R.; Khan, A.I.; Abushark, Y.B.; Alam, M.M.; Agrawal, A.; Khan, R.A. An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications. *IEEE Access* **2020**, *8*, 50944–50957. [[CrossRef](#)]
2. Steinbart, P.J.; Keith, M.J.; Babb, J. Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Inf. Syst. Res.* **2016**, *27*, 219–239. [[CrossRef](#)]
3. Florêncio, D.; Herley, C.; Van Oorschot, P.C. Password Portfolios and the {Finite-Effort} User: Sustainably Managing Large Numbers of Accounts. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, USA, 20–22 August 2014; pp. 575–590.
4. Al-Ameen, M.N.; Marne, S.T.; Fatema, K.; Wright, M.; Scielzo, S. On improving the memorability of system-assigned recognition-based passwords. *Behav. Inf. Technol.* **2022**, *41*, 1115–1131. [[CrossRef](#)]
5. Reuter, C.; Iacono, L.L.; Benlian, A. A quarter century of usable security and privacy research: Transparency, tailorability, and the road ahead. *Behav. Inf. Technol.* **2022**, *41*, 2035–2048. [[CrossRef](#)]
6. Distler, V.; Fassl, M.; Habib, H.; Krombholz, K.; Lenzini, G.; Lallemand, C.; Cranor, L.F.; Koenig, V. A systematic literature review of empirical methods and risk representation in usable privacy and security research. *ACM Trans. Comput.-Hum. Interact. (TOCHI)* **2021**, *28*, 1–50. [[CrossRef](#)]
7. Gaines, B.R. From facilitating interactivity to managing hyperconnectivity: 50 years of human–computer studies. *Int. J. Hum.-Comput. Stud.* **2019**, *131*, 4–22. [[CrossRef](#)]
8. Sae-Bae, N.; Wu, J.; Memon, N.; Konrad, J.; Ishwar, P. Emerging NUI-based methods for user authentication: A new taxonomy and survey. *IEEE Trans. Biom. Behav. Identity Sci.* **2019**, *1*, 5–31. [[CrossRef](#)]
9. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [[CrossRef](#)]

10. World Economic Forum. COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications. 2020. Available online: <https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-itsimplications> (accessed on 1 December 2022).
11. Lennartsson, M.; Kävrestad, J.; Nohlberg, M. Exploring the meaning of usable security—A literature review. *Inf. Comput. Secur.* **2021**, *29*, 647–663. [[CrossRef](#)]
12. Nwokedi, U.O.; Onyimbo, B.A.; Rad, B.B. Usability and security in user interface design: A systematic literature review. *Int. J. Inf. Technol. Comput. Sci. (IJITCS)* **2016**, *8*, 72–80. [[CrossRef](#)]
13. Zhang, R.; Xiao, Y.; Sun, S.; Ma, H. Efficient multi-factor authenticated key exchange scheme for mobile communications. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 625–634. [[CrossRef](#)]
14. Bicakci, K.; Kiziloz, H.E. Leveraging human computation for pure-text Human Interaction Proofs. *Int. J. Hum.-Comput. Stud.* **2016**, *92*, 44–54. [[CrossRef](#)]
15. Nehmadi, L.; Meyer, J. Effects of authentication method and system properties on authentication decisions and performance. *J. Cogn. Eng. Decis. Mak.* **2015**, *9*, 130–148. [[CrossRef](#)]
16. Shi, C.; Xu, X.; Ji, S.; Bu, K.; Chen, J.; Beyah, R.; Wang, T. Adversarial captchas. *IEEE Trans. Cybern.* **2021**, *52*, 6095–6108. [[CrossRef](#)]
17. Gao, S.; Mohamed, M.; Saxena, N.; Zhang, C. Emerging-image motion captchas: Vulnerabilities of existing designs, and countermeasures. *IEEE Trans. Dependable Secur. Comput.* **2017**, *16*, 1040–1053. [[CrossRef](#)]
18. Kiziloz, H.E.; Bicakci, K. A Closer Look at Pure-Text Human-Interaction Proofs. *IEEE Trans. Hum.-Mach. Syst.* **2016**, *47*, 994–1004. [[CrossRef](#)]
19. Xu, Y.; Reynaga, G.; Chiasson, S.; Frahm, J.M.; Monrose, F.; Van Oorschot, P.C. Security analysis and related usability of motion-based captchas: Decoding codewords in motion. *IEEE Trans. Dependable Secur. Comput.* **2013**, *11*, 480–493. [[CrossRef](#)]
20. Olalere, A.; Feng, J.H.; Lazar, J.; Brooks, T. Investigating the effects of sound masking on the use of audio captchas. *Behav. Inf. Technol.* **2014**, *33*, 919–928. [[CrossRef](#)]
21. Yan, J.; El Ahmad, A.S. Breaking visual captchas with naive pattern recognition algorithms. In Proceedings of the Twenty-Third Annual Computer Security Applications Conference (ACSAC), Miami Beach, FL, USA, 10–14 December 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 279–291.
22. Guerar, M.; Migliardi, M.; Merlo, A.; Benmohammed, M.; Palmieri, F.; Castiglione, A. Using screen brightness to improve security in mobile social network access. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 621–632. [[CrossRef](#)]
23. Khan, M.A.; Din, I.U.; Jadoon, S.U.; Khan, M.K.; Guizani, M.; Awan, K.A. G-RAT| a novel graphical randomized authentication technique for consumer smart devices. *IEEE Trans. Consum. Electron.* **2019**, *65*, 215–223. [[CrossRef](#)]
24. Chiasson, S.; Stobert, E.; Forget, A.; Biddle, R.; Van Oorschot, P.C. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Trans. Dependable Secur. Comput.* **2011**, *9*, 222–235. [[CrossRef](#)]
25. Biddle, R.; Mannan, M.; van Oorschot, P.C.; Whalen, T. User study, analysis, and usable security of passwords based on digital objects. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 970–979. [[CrossRef](#)]
26. Juang, K.; Greenstein, J. Integrating visual mnemonics and input feedback with passphrases to improve the usability and security of digital authentication. *Hum. Factors* **2018**, *60*, 658–668. [[CrossRef](#)] [[PubMed](#)]
27. Al-Ameen, M.N.; Wright, M. Exploring the potential of geopass: A geographic location-password scheme. *Interact. Comput.* **2017**, *29*, 605–627. [[CrossRef](#)]
28. MacRae, B.; Salehi-Abari, A.; Thorpe, J. An exploration of geographic authentication schemes. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1997–2012. [[CrossRef](#)]
29. Zhang, Y.; Han, D.; Li, A.; Zhang, L.; Li, T.; Zhang, Y. Magauth: Secure and usable two-factor authentication with magnetic wrist wearables. *IEEE Trans. Mob. Comput.* **2021**, *22*, 311–327. [[CrossRef](#)]
30. Mathis, F.; Williamson, J.H.; Vaniea, K.; Khamis, M. Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing. *ACM Trans. Comput.-Hum. Interact. (ToCHI)* **2021**, *28*, 1–44. [[CrossRef](#)]
31. Wazir, W.; Khattak, H.A.; Almogren, A.; Khan, M.A.; Din, I.U. Doodle-based authentication technique using augmented reality. *IEEE Access* **2020**, *8*, 4022–4034. [[CrossRef](#)]
32. Li, Y.; Cheng, Y.; Meng, W.; Li, Y.; Deng, R.H. Designing leakage-resilient password entry on head-mounted smart wearable glass devices. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 307–321. [[CrossRef](#)]
33. Khamis, M.; Marky, K.; Bulling, A.; Alt, F. User-centred multimodal authentication: Securing handheld mobile devices using gaze and touch input. *Behav. Inf. Technol.* **2022**, *41*, 2061–2083. [[CrossRef](#)]
34. Chakraborty, N.; Li, J.Q.; Mondal, S.; Luo, C.; Wang, H.; Alazab, M.; Chen, F.; Pan, Y. On designing a lesser obtrusive authentication protocol to prevent machine-learning-based threats in internet of things. *IEEE Internet Things J.* **2020**, *8*, 3255–3267. [[CrossRef](#)]
35. Hartwig, K.; Reuter, C. Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behav. Inf. Technol.* **2022**, *41*, 1357–1380. [[CrossRef](#)]
36. Alharbi, A.; Alharbi, T. Design and evaluation of an authentication framework for wearable devices. *IEEE Access* **2020**, *8*, 80369–80381. [[CrossRef](#)]
37. Perković, T.; Čagalj, M.; Mastelić, T.; Saxena, N.; Begušić, D. Secure initialization of multiple constrained wireless devices for an unaided user. *IEEE Trans. Mob. Comput.* **2012**, *11*, 337–351. [[CrossRef](#)]
38. Leguesse, Y.; Colombo, C.; Vella, M.; Hernandez-Castro, J. PoPL: Proof-of-Presence and Locality, or How to Secure Financial Transactions on Your Smartphone. *IEEE Access* **2021**, *9*, 168600–168612. [[CrossRef](#)]

39. Ali, M.; Baloch, A.; Waheed, A.; Zareei, M.; Manzoor, R.; Sajid, H.; Alanazi, F. A simple and secure reformation-based password scheme. *IEEE Access* **2021**, *9*, 11655–11674. [\[CrossRef\]](#)
40. 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. [\[CrossRef\]](#)
41. Weir, C.S.; Douglas, G.; Richardson, T.; Jack, M. Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interact. Comput.* **2010**, *22*, 153–164. [\[CrossRef\]](#)
42. Flechais, I.; Sasse, M.A. Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. *Int. J. Hum.-Comput. Stud.* **2009**, *67*, 281–296. [\[CrossRef\]](#)
43. Alsharnouby, M.; Alaca, F.; Chiasson, S. Why phishing still works: User strategies for combating phishing attacks. *Int. J. Hum.-Comput. Stud.* **2015**, *82*, 69–82. [\[CrossRef\]](#)
44. Roth, V.; Straub, T.; Richter, K. Security and usability engineering with particular attention to electronic mail. *Int. J. Hum.-Comput. Stud.* **2005**, *63*, 51–73. [\[CrossRef\]](#)
45. Gorski, P.L.; Möller, S.; Wiefeling, S.; Iacono, L.L. “I just looked for the solution!” On Integrating Security-Relevant Information in Non-Security API Documentation to Support Secure Coding Practices. *IEEE Trans. Softw. Eng.* **2021**, *48*, 3467–3484. [\[CrossRef\]](#)
46. Dhillon, G.; Oliveira, T.; Susarapu, S.; Caldeira, M. Deciding between information security and usability: Developing value based objectives. *Comput. Hum. Behav.* **2016**, *61*, 656–666. [\[CrossRef\]](#)
47. Alemerien, K. User-friendly security patterns for designing social network websites. *Int. J. Technol. Hum. Interact. (IJTHI)* **2017**, *13*, 39–60. [\[CrossRef\]](#)
48. Merdenyan, B.; Petrie, H. Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours. *Behav. Inf. Technol.* **2022**, *41*, 2514–2527. [\[CrossRef\]](#)
49. Haque, S.T.; Wright, M.; Scielzo, S. Hierarchy of users’ web passwords: Perceptions, practices and susceptibilities. *Int. J. Hum.-Comput. Stud.* **2014**, *72*, 860–874. [\[CrossRef\]](#)
50. Hirschprung, R.S.; Tayro, S.; Reznik, E. Optimising technological literacy acquirement to protect privacy and security. *Behav. Inf. Technol.* **2022**, *41*, 922–933. [\[CrossRef\]](#)
51. Gopavaram, S.R.; Bhide, O.; Camp, L.J. Can You Hear Me Now? Audio and Visual Interactions That Change App Choices. *Front. Psychol.* **2020**, *11*, 2227. [\[CrossRef\]](#)
52. Gates, C.S.; Chen, J.; Li, N.; Proctor, R.W. Effective risk communication for android apps. *IEEE Trans. Dependable Secur. Comput.* **2013**, *11*, 252–265. [\[CrossRef\]](#)
53. Chen, J.; Gates, C.S.; Li, N.; Proctor, R.W. Influence of risk/safety information framing on android app-installation decisions. *J. Cogn. Eng. Decis. Mak.* **2015**, *9*, 149–168. [\[CrossRef\]](#)
54. Wu, D.; Moody, G.D.; Zhang, J.; Lowry, P.B. Effects of the design of mobile security notifications and mobile app usability on users’ security perceptions and continued use intention. *Inf. Manag.* **2020**, *57*, 103235. [\[CrossRef\]](#)
55. Alshamsi, A.; Andras, P. User perception of Bitcoin usability and security across novice users. *Int. J. Hum.-Comput. Stud.* **2019**, *126*, 94–110. [\[CrossRef\]](#)
56. Zhang, J.; Luximon, Y. Interaction design for security based on social context. *Int. J. Hum.-Comput. Stud.* **2021**, *154*, 102675. [\[CrossRef\]](#)
57. Mohamed, M.A.; Chakraborty, J.; Dehlinger, J. Trading off usability and security in user interface design through mental models. *Behav. Inf. Technol.* **2017**, *36*, 493–516. [\[CrossRef\]](#)
58. Al-Zahrani, F.A. Evaluating the usable-security of healthcare software through unified technique of fuzzy logic, ANP and TOPSIS. *IEEE Access* **2020**, *8*, 109905–109916. [\[CrossRef\]](#)
59. Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Baz, M.; Agrawal, A.; Khan, R.A. A hybrid model of hesitant fuzzy decision-making analysis for estimating usable-security of software. *IEEE Access* **2020**, *8*, 72694–72712. [\[CrossRef\]](#)
60. Di Nocera, F.; Tempestini, G. Getting Rid of the Usability/Security Trade-Off: A Behavioral Approach. *J. Cybersecur. Priv.* **2022**, *2*, 245–256. [\[CrossRef\]](#)
61. Bravo-Lillo, C.; Cranor, L.; Komanduri, S.; Schechter, S.; Sleeper, M. Harder to ignore? Revisiting {Pop-Up} fatigue and approaches to prevent it. In Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, USA, 9–11 July 2014; pp. 105–111.
62. Bravo-Lillo, C.; Komanduri, S.; Cranor, L.F.; Reeder, R.W.; Sleeper, M.; Downs, J.; Schechter, S. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle, UK, 24–26 July 2013; pp. 1–12.
63. Bhana, B.; Flowerday, S.V. Usability of the login authentication process: Passphrases and passwords. *Inf. Comput. Secur.* **2022**, *30*, 280–305. [\[CrossRef\]](#)
64. Gutfleisch, M.; Klemmer, J.H.; Busch, N.; Acar, Y.; Sasse, M.A.; Fahl, S. How Does Usable Security (Not) End Up in Software Products? Results from a Qualitative Interview Study. In Proceedings of the 43rd IEEE Symposium on Security and Privacy (S&P), San Francisco, CA, USA, 22–26 May 2022; IEEE: Piscataway, NJ, USA, 2022.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.