How to design browser security and privacy alerts

Lynsay A. Shepherd
Karen Renaud

This is the accepted manuscript of the conference paper:


How to Design Browser Security and Privacy Alerts

Lynsay A. Shepherd  
School of Design and Informatics  
Abertay University  
Dundee, United Kingdom  
lynsay.shepherd@abertay.ac.uk

Karen Renaud  
School of Design and Informatics  
Abertay University  
Dundee, United Kingdom  
k.renaud@abertay.ac.uk

ABSTRACT
It is important to design browser security and privacy alerts so as to maximise their value to the end user, and their efficacy in terms of communicating risk. We derived a list of design guidelines from the research literature by carrying out a systematic review. We analysed the papers both quantitatively and qualitatively to arrive at a comprehensive set of guidelines. Our findings aim to provide designers and developers with guidance as to how to construct privacy and security alerts. We conclude by providing an alert template, highlighting its adherence to the derived guidelines.

ACM Reference Format:
https://doi.org/10.1145/nnnnnn.nnnnnn

1 INTRODUCTION
It is non-trivial to design effective alerts in the security and privacy domain.
Browser designers do their best to inform users about security-related aspects as they surf the web. Owing to the number of potential pitfalls, this means end users can be bombarded with security alerts [2], and users often ignore them [8, 33]. Developers sometimes make unfounded assumptions about the background knowledge of alert recipients [30], which can make the alerts incomprehensible.
Privacy alerts also have flaws, both in terms of content and delivery [35]. Users are often overwhelmed by these alerts because there are too many [21], or because they do not know what actions to take as a consequence [56].

This diminishes the impact of alerts, and leaves users vulnerable to unknowingly carrying out actions which will compromise their privacy or security.

Traditional usability guidelines cannot necessarily be used “as-is” in the security and privacy context. This is because neither privacy nor security are the end user’s primary task [11, 32]. Alerts interrupt the user’s pursuit of their primary goal and are thus often perceived to be a nuisance [5]. We therefore need specific guidelines to inform alert design in the security and privacy context.

Much has been written about alert design, highlighted by the following sections. Yet one can hardly expect busy deadline-driven software engineers, the very people who are producing these alerts, to keep up with the latest research.
We therefore performed a systematic literature review to consolidate all the published guidelines into one coherent list (Section 3). Previously, Bauer et al. [13] presented a list of warning design guidelines in 2013. Our work provides an updated, more comprehensive, list of guidelines, specifically tailored towards browser-based alerts.
Having derived a comprehensive set of guidelines, we realised that merely providing a list of guidelines is not an optimal way of supporting designers. Luger and Rodden [38] argue that such lists of guidelines are unlikely to be followed in the pressured environment of software development and design. Moreover, some of the published guidelines conflict [39], which is unhelpful.
To make our consolidated guidelines as helpful as possible, we decided to convey the spirit, rather than the letter, of the guidelines in the form of an example alert template (Section 4). This conveys the “how” of alert design, rather than the “what”, encapsulated in a linear set of alert guidelines. Future work is explored in Section 5, and we conclude in Section 6.

2 INFORMING END USERS
First we clarify the nomenclature used in this paper. We then provide an overview of the human in the loop model of human information processing. We conclude by explaining the difference between the foundational security and privacy concepts.
2.1 Nomenclature
We investigated guidelines that inform the design of warnings, alerts, notifications, prompts or provision of feedback. The underlying concept is the same: provision of important information to an end user that the system considers he or she should be apprised of. We shall use the term ‘alert’ as a unifying term to represent all the terminologies used by papers cited in this paper.

2.2 Human Information Processing
Wogalter and Mayhorn [63] explain that warnings (what we call alerts) are a type of risk communication. Wogalter [64] explains that warnings have two purposes: (1) communicate information, and (2) reduce unwise behaviours. To achieve these aims the warnings have to be designed carefully. The Web Content Accessibility Guidelines can also be applied to alerts [7] i.e. that they should be perceivable, operable, understandable and robust.

Shannon [57] and Lasswell [36] both proposed models of human communication which help us to understand how humans process alerts.

Wogalter, Defjoy, and Laughery [65] developed the C-HIP model in the context of warning research. Their model builds on the work of Shannon and Lasswell and can be considered to be somewhat unrealistic because it does not include a noise component. In a world of noisy communication, such a model is incomplete. Cranor [17] proposed a ‘human-in-the-loop’ framework which is more comprehensive and reflects the factors impacting communications in the context of privacy and security alerts.

2.3 Security vs. Privacy
It is important to realise that security and privacy are fundamentally different concepts. Skinner et al. [59] argue that a secure information system does not necessarily imply that privacy will be preserved in the system. Gritzalis and Lambrinoudakis [24] make the distinction between privacy and security as follows: “a piece of information is secure when its content is protected, it is private when the identity of the owner is protected”. As an example, they refer to a company that collects customer information, and stores it in an encrypted format. This ensures that the information is secured. Yet the same company may sell the information to another company, thereby violating the owners’ privacy.

Bambauer [12, p. 667] explains: “Privacy discourse involves difficult normative decisions about competing claims to legitimate access to, use of and alteration of information.” Security, on the other hand, is “the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.” [20].

Privacy and security are clearly distinct concepts, but their alerts still share some common characteristics in that they exist to tell the end user to something important. We therefore present three lists of guidelines: (1) generic, (2) privacy-specific, and (3) security-specific.

3 CONTEMPLATING THE ALERT LITERATURE
We decided to focus on browser alerts firstly because of the popularity of web applications [41] such as email, claimed to be the most popular application in use [5] and video streaming [31]. The second reason is that browsers run on all devices, ranging from Desktops to Smartphones. We felt that our guidelines could be maximally useful to developers if we focused on guidelines for browser alerts.

We carried out a systematic literature review, as advised by [50]. The literature search was carried out between November and December 2017 as follows:

Databases: ACM, Springer, Web of Science, Scopus, IEEE, and then Google Scholar to identify publications that did not appear in the other databases.

Keywords: ‘design guidelines’ and ‘browser’ and (‘security’ or ‘privacy’) and (‘feedback’ or ‘warnings’ or ‘alert’ or ‘notification’)

Time Range: 2007—2017

Exclusion Criteria: Patents, citations, non-peer reviewed, not English or unobtainable.

3.1 Quantitative analysis
One particular measure of activity in a research field is the number of papers published over the decade in question.
Figure 2 shows the number of papers, and also how many times the papers have been cited up to the date we carried out our literature review.

It is interesting to note that 25 of the 72 papers had no citations at all. The average number of citations is 7.38, the mode is 0, and the median is 2. Only four of the papers had been cited by more than 50 other publications. The top two most-cited publications appeared in conferences and the third most-cited publication appeared in a journal.

Figure 3 shows the citations for papers in each of the paper focus areas. The top cited paper is a security paper, with the next two most-cited papers being in the privacy area.

3.2 Qualitative analysis

We analysed the guidelines using Thematic Analysis [25]. This approach supports pinpointing, examining, and recording themes that emerge from the papers. We commenced by familiarising ourselves with the papers. We then generated initial codes and searched for themes as we collated these codes. We then reviewed the themes, defining and naming them.

Some of the guidelines applied equally to privacy and security, but others were clearly specific to either privacy or security. This is not unexpected because, as argued earlier, privacy and security are fundamentally different concepts. We shall thus present generic guidelines first, then concept-specific guidelines separately, reflecting the fundamental differences between the two concepts.

3.3 Generic Guidelines

We report first on the generic themes that coincide with Cranor’s framework [17], depicted in Figure 1.

Communication Impediments (CI). Here mitigations to ameliorate the effects of impediments should be included. For example, provide users with the means to recover from hasty decisions [29].

Personal Variables & Capabilities (PV). Some users may have low numeracy levels. Instead of providing them with figures regarding risk, perhaps utilise emotions or mood. Similarly, users may have different understanding of visuals [45]. Only by testing can the efficacy of these be confirmed.

Communication Delivery (CD). Human attention is a finite resource [16]. Do not squander it, and do not expect the recipient to give you any as a matter of course.

CD1: Modality — Murphy-Hill & Murphy [42, 62] suggest that pictures be used to ease communication. When delivering warning alerts, users prefer text and graphical-based information, rather than auditory information[15].
On the other hand, Goldberg [23] suggests that text should be used exclusively. This might be to maximise accessibility, and the middle road would be to ensure that alt text is provided for all images.

Work conducted by Anderson et al. [9, 10] notes the use of polymorphism in warning alerts to reduce habituation.

**CD2: Timing** — If alerts appear too often, the recipients may get annoyed and start ignoring them [4, 42]. Alerts should be issued only when necessary, to avoid irritating the user [61].

Westermann [62] found that people were most annoyed by alerts if they are busy with a task, especially when the task is complex, but less annoyed in between tasks or when they were waiting for something.

It is important to prioritise the warnings so that only the most important ones merit immediate interruption [4, 62].

**CD3: Location** — Westermann [62] considers alert location to be important. Many browsers, for example, display alerts either in the address bar (padlock and the word ‘Secure’ in Chrome), or at the bottom of the screen. These are easily missed by users. If we want people to notice the alerts it ought to be displayed where they are currently focusing their attention. In particular [4] point out that passive toolbar-located warnings are less effective than full page warnings. Pala and Wang [48] also suggest alerts should be placed where the users are focusing their attention. In the study conducted by Chen, Zahedi, and Abbasi, users preferred alerts to be placed in the centre of the screen [15].

**CD4: Appearance** — Kelley [32] provides a number of recommendations: (1) the alert should be surrounded by a box to clearly demarcate it; (2) provide a title to facilitate speedy recognition. Be careful with colour use so as not to disadvantage those with colour deficiencies [23]. A neutral grey colour can be used for the background of alerts, as it is unlikely to annoy the user [61].

**Communication Processing (CP).**

**CP1: Make Essential Information Pertinent** — Lin [37] suggests highlighting the most important information. Keep initial details about the risk to a minimum [45, 46]. Only the most important information should be displayed to the user immediately with links to more information should they want it [61]. The granularity of information is important. Wordy information will not be read, and information that is too condensed can be obscure. In providing alerts, a balance must be found [11].

**CP2: Maximise Understandability and Consistency** — Alerts should maximise understandability [32, 42, 55, 62], and should be presented in a consistent format [7, 42]. Provide concrete explanations [47]. The importance of this aspect is confirmed by [44]. Keep explanations simple [37]. Acronyms and jargon should be avoided and the use of meaningful terminology encouraged [11, 32, 55, 58]. Separate semantically different kinds of information [32, 60].

Presented text should be easy for users to comprehend [61]. Short, simple sentences, devoid of complex grammatical structures, should be used. The use of technical words should be avoided (i.e. words listed in the indexes of IT security books) [18, 26, 27, 48]. Unclear alerts are more likely to be ignored, and consideration should be given to the exact meanings of words used [45].

Work by Bravo-Lillo et al. [14] investigated the use of redesigned warning alerts. Longer warning alerts performed poorly in user testing, suggesting users may have become confused. Although existing work highlights that shorter alerts are most effective at communicating security warnings to the user, the challenge of delivering such alerts whilst providing the user with enough text to foster understanding has been acknowledged [22].

**Application (AP).**

**AP1: Be Specific** — Bravo-Lillo et al. [14] state that “to be successful, warnings should both motivate a user to respond, and help users understand the risk, in that order”. Always tell the users what actions to take, if indeed they should take action [7, 29].

**AP2: End Goal** — Consider the way in which you want to communicate a risk to the user e.g. is the alert to draw them away from a risky situation, or is the alert to help them to understand the risk [45]?

**AP3: Effort Does Not Deter** — Akhawe and Felt [4] explain that designers should not use the number of clicks required to bypass a warning to deter users. Their study showed that users were not sensitive to the number of clicks once they had made a decision.

**Intentions (IN).**

It is important to note that delivering warnings is worthwhile. Silic et al. [58] found that people took note of displayed warning messages, suggesting that they thought about the information before making the decision to proceed. If people are reading and thinking about messages, these messages have a chance of changing attitudes and beliefs.

Vasalou [60] says alerts should give recipients “space for interpretation”, so that they can interpret the information as it applies to themselves personally.

Phrasing of alerts could be personalised, depending on the user’s skill level, and experience [15, 45, 46]. Personalised alerts were said to be successful when used to inform users about two-factor authentication, and bullet-points can be used to aid clarity of information presented [32].

It is important for the user to retain a level of control [29, 60, 66]. Schaub et al. [54] distinguish between three levels of user control: (1) blocking, (2) non-blocking and (3)
decoupled. A designer has to decide whether the user has to acknowledge the message (blocking) or not (non-blocking), whether they can defer it (decoupled), or whether it will expire after displaying for a certain period of time [42].

Users should be provided with the option to respond to a risk they have been alerted to, and helped to visualise potential consequences [45]. Work by Volkamer et al. [61] concurs that the potential consequences of a risk should be conveyed to the user, along with potential recommendations.

Make sure the user can easily get in touch with someone to ask about warning-type alerts [23]. Contact information should be conspicuously placed so worried users will be able to get help [29].

3.4 Privacy-Specific Guidelines

Allow users to make privacy choices that are (1) meaningful, (2) informed, (3) timely [16].

**P-CI: Inspire Trust** — Trust should be deliberately built and maintained [42] by framing the privacy alert very carefully [3]. Rather counter-intuitively, privacy alerts should not provide justifications for information requests. Researchers report that justifications potentially reduce the end-user’s trust in the system [1, 3, 34, 51].

**P-PV: Privacy Expectations** — Lin [37] points out that users have different privacy expectations, and that an alert interface should reflect this reality.

**P-CD: Specificity** — Ensure that the sensitivity of the data is communicated to the user [43].

**P-IN: Enhance Control** — Ensure that control resides with the user [43]. Do not merely report that some privacy invasion has occurred: allow the user to control disclosure. It is necessary to balance the number of interruptions with ensuring that the user retains a sense of control [16].

People have different levels of privacy concerns, and the alerts should afford users the level of control matching their personal privacy concerns.

3.5 Security-Specific Guidelines

Herzog and Shahmehri [28] highlight the importance of security features in applications, stressing that “security is rarely the primary user task”.

**S-CI: Context-Sensitive Help** — Constantly visible context sensitive help may prove useful in helping the user understand security. Help may be provided via the use of an agent [28]. The user should be provided with the option to find further information in a contextually-aware setting [46, 48].

**S-CD1: Provide Justification** — The user needs to know why the alert is being provided [42]. Provide information as to whether a component is secure or insecure. By displaying this information in either case, this provides a consistent interface for the user [48]. Ensure that the current state of the system is displayed to the user [46].

**S-CD2: Colour** — Research regarding two-factor authentication suggests the use of blue as a peaceful colour. Red might indicate an incident has occurred [15, 52]. Felt et al. [22] suggest utilising “opinionated design”. For example, make the “correct” response the more visually appealing option e.g. the button should have a high contrast level against the background. Others have utilised green as colour, noting that it is seen as safe. Whilst users should be given options regarding how to proceed with their tasks, it has been suggested that placing the “correct” option in green serves to guide users towards the safe choice [61]. Where colourblind users may have issues with warnings, the use of secondary information (icons) can convey the same message [61].

**S-CD3: Graphics** — In one study, participants felt the inclusion of graphics in an alert about two-factor authentication conveyed a tone which was less serious, and suspicious [52]. Conversely, other studies conclude graphics are required in alerts, to convey reassurance, draw attention, and to reduce cognitive effort [61]. This is a prime example of conflicting guidelines.

Eargle [19] suggests that facial expressions could be used to convey threat levels in security alerts but this has not been confirmed by any other studies in our studied group.

**S-IN: Control Level** — If a security issue is detected on a page, users would prefer the security alert to block them from visiting a malicious website [15]. Other research stated the final security decisions should be left to the user, though users should be provided with alternative options on how to proceed with their task [61].

4 INFORMING DESIGNERS

The previous section provided a list of recommendations for designing alerts. In Figure 4, the solid black boxes denote privacy guidelines (prefixed with ‘P’), whilst the grey-scale boxes denote security guidelines (prefixed with ‘S’). Privacy and security guidelines include communication impediments (P-CL, S-Cl), communication delivery (P-CD, S-CD), personal variables (P-PV), and intentions (P-IN, S-IN).

However, as pointed out by [53], and confirmed by [38], designers have difficulty benefiting from these kinds of flat lists of guidelines.

Luger and Rodden’s [38] designers spoke about the value of examples in encapsulating the lessons of design guidelines in a more palatable format. We thus present a template in Figure 5, and explain how it satisfies the guidelines, extending the initial template produced by Bauer et al. [13].
4.1 Development Good Practice

Creating a well-designed environment can aid in establishing trust [40]. Moreover, it is important to ensure that people are receptive to alerts [62]. The best way to confirm both trustworthiness and alert receptiveness is by means of thorough testing [29]. Options are A/B testing in the wild, controlled experiments, field studies [4], or case studies post-deployment [42].

5 FUTURE WORK

The systematic literature review identified a lack of research surrounding the optimal placement of security and privacy alerts within the web browser. Whilst work carried out by Chen, Zahedi, and Abbasi [15] showed users preferred alerts in the centre of the screen, usability studies have shown there are a variety of patterns users exhibit when browsing web content [49]. This suggests that further research is required into the optimal placement of security and privacy alerts.

It is also interesting to note from Figure 4 that there are no security or privacy-specific guidelines in terms of Communication Processing or Application. Furthermore, few of the papers returned in the systematic literature review mentioned consistency of alert design. These are certainly areas for further investigation.

Several guidelines gathered from literature conflict, and this issue has been highlighted by other guideline papers [53]. Previous research has acknowledged that “Not all best practices can be simultaneously satisfied”; therefore, trade-offs must occur [22]. Masip et al. [39] have investigated the development of a design process to assist with design choices when there are potentially conflicting user interface guidelines. In the future, we plan to develop a methodology for prioritising the guidelines to support security and privacy alert design.
6 CONCLUSION

The systematic review process highlighted a large proportion of the work found online relating to alerts were sourced from student theses (both at Masters and PhD level). Whilst conducting the analysis process, it became clear that some alert guidelines were developed for security, and others were developed for privacy. These seemed, in many cases, to be fundamentally different, suggesting that different guidelines are required for these two distinct areas.

We publish this work as a first attempt to provide guidance to designers and developers who need to incorporate alerts into their systems. In the future, we seek to prioritise the guidelines, addressing the issue of potential conflicts, and with feedback from practitioners, iteratively refine the guideline list.

REFERENCES


