



Warning users about cyber threats through sounds

Prerit Datta¹ · Akbar Siami Namin¹ · Keith S. Jones² · Rattikorn Hewett¹

Received: 9 January 2021 / Accepted: 18 June 2021

Published online: 29 June 2021

© The Author(s) 2021

Abstract

This paper reports a formative evaluation of auditory representations of cyber security threat indicators and cues, referred to as sonifications, to warn users about cyber threats. Most Internet browsers provide visual cues and textual warnings to help users identify when they are at risk. Although these alarming mechanisms are very effective in informing users, there are certain situations and circumstances where these alarming techniques are unsuccessful in drawing the user's attention: (1) security warnings and features (e.g., blocking out malicious Websites) might overwhelm a typical Internet user and thus the users may overlook or ignore visual and textual warnings and, as a result, they might be targeted, (2) these visual cues are inaccessible to certain users such as those with visual impairments. This work is motivated by our previous work of the use of sonification of security warnings to users who are visually impaired. To investigate the usefulness of sonification in general security settings, this work uses real Websites instead of simulated Web applications with sighted participants. The study targets sonification for three different types of security threats: (1) phishing, (2) malware downloading, and (3) form filling. The results show that on average 58% of the participants were able to correctly remember what the sonification conveyed. Additionally, about 73% of the participants were able to correctly identify the threat that the sonification represented while performing tasks using real Websites. Furthermore, the paper introduces "CyberWarner", a sonification sandbox that can be installed on the Google Chrome browser to enable auditory representations of certain security threats and cues that are designed based on several URL heuristics.

Article highlights

1. It is feasible to develop sonified cyber security threat indicators that users intuitively understand with minimal experience and training.
2. Users are more cautious about malicious activities in general. However, when navigating real Websites, they
- are less informed. This might be due to the appearance of the navigating Websites or the overwhelming issues when performing tasks.
3. Participants' qualitative responses indicate that even when they did not remember what the sonification conveyed, the sonification was able to capture the user's attention and take safe actions in response.

Keywords cyber security · Sonification · Formative evaluation · Web security

✉ Prerit Datta, prerit.datta@ttu.edu; Akbar Siami Namin, akbar.namin@ttu.edu; Keith S. Jones, keith.s.jones@ttu.edu; Rattikorn Hewett, rattikorn.hewett@ttu.edu | ¹Department of Computer Science, Texas Tech University, Lubbock, TX 79409, US. ²Department of Psychological Sciences, Texas Tech University, Lubbock, TX 79409, US.



1 Introduction

Data breaches are of growing concern to organizations. According to the Symantec Annual Threat Report published in 2017 [1], over 7.1 billion identities have been exposed as a result of data breaches. Targeted attacks on organizations went up by 10% in 2017. Due to increase of cyber attacks, there was a significant rise in spear-phishing emails (about 71%) and new malware variants (87.7%) in 2018 [2]. As per Thales Global Security report published in 2018 [3], about 36% of major organizations in the world experienced some form of a data breach, while United States alone had over 46% of data breaches in the past year - the highest in the world.

1.1 Motivation: the role of human errors and security fatigue

According to the IBM Threat Intelligence Index Report published in 2018, close to two billion records were exposed as a result of human errors due to incorrect configurations or permissions [4]. The incidents caused by human mistakes vary from being a victim of phishing attacks to visiting malicious Websites, spreading viruses, and information disclosure of sensitive information.

Current Internet browsers offer a good number of functional features to effectively represent security warnings. Most of the newest versions of major browsers, such as Internet Explorer (IE), Firefox, Safari, and Google Chrome aim to protect users not only against traditional security vulnerabilities but also malware and phishing attacks. These browsers also enable users to browse the Internet anonymously and in private sessions and even block known malicious Websites.

Security warning messages have been re-phrased and simplified to inform users about potential risks and dangers. In addition to the textual description and communications, some visualization approaches have also been introduced to offer adequate information for users without overwhelming them with unnecessary technical details [5]. However, despite such built-in measures, the Internet remains a ripe place for cyber attacks.

A recent study conducted by National Institute of Standard and Technology (NIST) [6] analyzed the online behavior of users in making security decisions. The study postulates that “*Security Fatigue*” is a phenomenon that causes people to make irrational security decisions as a result of constantly trying to be careful online. The participants of study expressed their frustration and anger of having to keep track of a multitude of security measures to avoid being locked out of their accounts and the constant alerts from the firewalls and antivirus software

installed on their systems. As people become constantly overwhelmed with warnings and notifications, they become desensitized to important alerts and start finding workarounds that could lead to catastrophic errors or incidents. This can be explained due to the fact that continuous decision-making can be taxing to the cognitive capabilities of humans to process everything at the same time and thus when it reaches saturation or threshold, it leads to “*burnout*” [7].

One of the lead causes of security fatigue is the need for strict compliance with security policies of the organizations [8, 9]. Some of the examples include encryption, automatic updates, and adhering to access-control policies [10]. Additionally, unsafe behaviors caused by security fatigue are exacerbated by an individual’s perceived level of risk and risk-avoidance [11]. While researchers have tried to measure and model security fatigue [7, 9], the mitigation of security fatigue is even more challenging.

Security warning messages are usually conveyed to users through their visual senses. While communication through visual perception is still the primary means for exchanging and conveying information, it is also possible that users may be overwhelmed with the huge number of visual effects and textual descriptions. Thus, some of the critical messages might be overlooked or missed by the users, and thus the underlying system and its users might be in danger or exposed to serious risk.

1.2 Contributions

In their earlier work (i.e., a formative evaluation) the authors introduced the idea of representing cyber threats and cues through auditory indicators, and thus utilizing the hearing sense as a new channel to communicate security risks to end-users [12, 13]. In that work, the authors introduced a systematic approach to sonify security threat indicators for a small set of security attacks namely phishing, downloading, and form-filling. To do so, the authors created a set of natural sounds to represent each security. For instance, the sound of a fishing rod was used to represent phishing attacks; whereas a sound effect for dropping a bomb warned users about a malware download.

The motivation for the authors’ earlier work [12, 13] was centered on the problem of Internet navigation for users who are visually impaired. Users with visual impairment may need better assistive technologies to help them navigate the Internet safely. Given the fact that users with visual impairments utilize their hearing senses in communication heavily, auditory warnings about security threats and cues were designed and tested. The results indicated the effectiveness of such an approach for making security was more usable for this kind of user.

In the present work, we conducted a formative evaluation of the use of sonifications with sighted participants (i.e., users without visual impairments) and hypothesize that the introduced technology can be useful and effective not only for visually impaired users but also for Internet users who do not have visual impairments. It should be noted that the current evaluation is not intended as a replacement to visual warnings but rather these two modalities may be used in tandem to offer more secure systems to the end-users. The key contributions of this paper are as follows:

1. Investigating the effectiveness of representing security threats and cues using natural sounds (i.e., auditory icons).
2. Conducting a formative evaluation of sonification artifacts to examine whether the users who are without visual impairment a) could correctly identify the cyber security threat that a given indicator was meant to convey, b) felt that each indicator sounded pleasant, urgent, and distinctive from background sounds, and c) could distinguish the best indicators for each cyber security threat from one another.
3. Introducing a sonification sandbox, called *CyberWarner*, that implements the security sonification for a number of security threats and cues. The tool enables other researchers to replicate the case studies and validate other forms of sonifications. The tool can be installed on the Google Chrome browser and alarm users about potential danger and risks associated with some major cyber threats and indicators.

It should be noted that the introduced sandbox, is a work-in-progress prototype to test and demonstrate the feasibility of the proposed methodology and the sonifications used in the study. Through the use of the sandbox, we try to represent major security events through sounds to reduce cognitive workload by drawing users' attention.

The rest of this paper is organized as follows: Sect. 2 provides the state-of-the art of text warning and use of sonification in warning users. Section 3 reports the results of a formative evaluation in which the designed sonifications were tested with Internet users who were not visually impaired. Section 4 introduces *CyberWarner*, which is an automated sonification sandbox prototype tool developed for enabling sonification on the Google Chrome browser. Section 5 presents the results of the current formative evaluation and highlights commonalities and differences across the two sets of participants, i.e., users who were and were not visually impaired. Section 6 discusses the conclusions drawn from the research and highlights future research directions.

2 State-of-the-art: security warning and sonification

This section presents an overview of the state-of-the-art in security warning and sonification literature.

2.1 Text-based security warnings

Cambridge dictionary defines a *warning* as a "notice of a possible danger or problem so that it can be *prevented* or *avoided*." A security warning is an alarm about something that may harm or compromise the protection of a system. Researchers have been studying the users' behavior and response to the security warnings in Web browsers to improve its effectiveness. Apart from the general technical problems such as date/time mismatch and antivirus alerts [14], security warnings can be triggered by visiting malicious Websites that may download malware or cause phishing attacks by spoofing popular Websites.

Egelman et al. [15] designed an experiment to study participants' behavior when presented with security warnings in the browser caused by spear-phishing attacks. Participants were not informed about the true nature of the study but were rather recruited to participate in a study about online shopping. The authors concluded that many of the participants ignored the warnings mainly because either they had encountered a similar-looking warning message before on a trusted Website or that they believed the warning was shown in error because of the temporal context of receiving the email shortly after placing the order. As an implication of the study, security warnings should look significantly different from general browser warnings and they should interrupt user's current tasks and ask them about their choice, thereby grabbing their attention.

Researchers have also studied if there is a significant difference in users' behavior when responding to security warnings across different Web browsers. Particularly, researchers have found that users tend to ignore browser warnings in Google Chrome more than Firefox [16]. The main reasons for differences in users' behavior are due to 1) better design of the warnings in Firefox browser [17] and also, 2) because Google Chrome has more users than Firefox [18]. Researchers have found that users often ignore the SSL warning messages in the browser when visiting Websites that look familiar to them. Based on their previous experience with these Websites, users tend to develop a sense of trust over time and thus ignore the warnings as they believe it must have occurred in error [18]. This behavior is dangerous as an attacker may easily spoof a Website and thus, a user may reveal confidential information when

interacting with the malicious Website thinking into believing that the malicious Website was real despite any SSL warnings issued by the browser.

In addition to looking into users' behavior across different Web browsers, researchers have also analyzed the effect of different security cues, icons, background colors, text description, gender, and age in security warnings. Egelman et al. [19] conducted a study to analyze the effects of adding a different text and a border color compared to the default security warnings in the Microsoft Internet Explorer. The authors found that even though the participants spent significantly more time reading the modified versions of the security warnings, these changes did not have any effect on the user's decision to heed to warning. The authors attribute this observation to the nature of lab studies that cause the participants to indulge in more risky behaviors than they normally would as the participants deem the lab environment to be "safer" as is also reported by a similar study [20].

To mitigate the inaction due to the habituation of security warnings, researchers have proposed the use of security warnings that dynamically change their appearance or animate to force the user to pay attention and choose the appropriate response to the warning presented. These warnings are known as *polymorphic warnings* [21–23]. Besides polymorphic warnings, Raja et al. [24] demonstrated the use of metaphors to visualize firewall warnings to improve comprehension to encourage safe behavior among users. The authors use images of a burglar trying to break into a house as a warning when an adversary is trying to break into the network. Although, visualization may improve the understanding of the immediate security problem, choosing appropriate images that convey the intended meaning is a challenging task. If not chosen carefully, the warning may be misunderstood by the users. Habituation remains a challenging issue when it comes to the security warning.

2.2 The use of sonification in warning

Sonification is the use of non-speech sounds to notify that some event has occurred. The use of sonification has been applied to a myriad of application domains. As a warning system in the domain of computer science, sonification finds its applications in sonifying anomalies by monitoring the network traffic [25–29] and improving situational awareness [30]. In addition, it has also been used in process monitoring to sonify malicious processes [31] and also in intrusion detection systems [32, 33] to alert the network administrators of any imminent threats.

Minakawa et al. [34] proposed a custom security warning system that uses an image of an animated puppy with

a bark sound to capture users' attention in dialog boxes. The authors reported that the Kawaii effect was able to capture users' attention, however, it necessarily did not stop them from visiting the malicious links. The authors attribute this to the bias in the study as the participants suspected the true nature of the study as discovered in the exit interviews.

While the use of abstract/synthetic sounds, also known as "earcons" [35–37] and speech sounds, has been widely studied for interface design in Human-Computer Interaction (HCI) and computer networking domain, the use of natural sounds or "auditory icons" [38] has not received enough attention in the cyber security domain. In this paper, we conducted a formative evaluation of the use of auditory icons (sounds that are natural and easily recognizable) with sighted participants who are not visually impaired to analyze the feasibility of such an approach in the cyber security domain (described in Sect. 3).

3 A formative evaluation of sonification for sighted users

According to a technical report published by the University of Wisconsin (2008) [39], some of the assistive technologies specifically designed for people with disabilities could be useful both for people with and without disabilities. For instance, according to the researchers at the University of Wisconsin, "students with hearing, visual, physical, psychiatric, learning or other disabilities can use screen magnifiers, and other assistive technologies to help them be more successful academically."

To perform a formative evaluation of sonifications for users who are not visually impaired the following questions arise:

- Do users without visual impairment, who utilize both visual and hearing senses, interpret the sonification technology and the representative sounds similar to users who are visually impaired?
- Does visiting real Websites and different application domains that were used for users with visual impairment change the perception of sonification for security threats? Research indicates that people rely on peripheral cues to assess the credibility of Websites [40]. It will be useful to study whether the appearance of Websites to users who are or not visually impaired may change the impact of security decision.

These motivating questions encouraged the authors to develop a sonification sandbox prototype tool, called *CyberWarner* (See Sect. 4). The sonification tool examines the use of auditory icons in grabbing the users' attention

with the presence of distractor tasks—which do not lead to any sonifications being played. This is described in the following sections.

3.1 Participant recruitment and study design

The evaluation involved 26 college students (18 males and 8 females) who were not visually impaired. 61.5% of the participants' rated themselves to be 19 years old or younger, while 38.5% participants' reported being in the 20–29 years age group. 23.1% of the participants rated their knowledge of using computing devices (such as computers, smartphones, etc.) as very good, while 46.2% and 30.8% rated their knowledge to be good and average, respectively.

Based on our formative evaluation, the testing consisted of two phases: (1) Out of Context, and (2) In Context. The "Out of Context" testing involves participants listen to sounds (i.e., sonification) designed for each cyber threat without considering any context or functional scenarios; whereas, "In Context" testing involves testing sonification in some business and functional tasks (e.g., visiting a banking Website) where the sonification is triggered upon observing a cyber threat. The participants were asked to sign an IRB-approved consent form prior to the study. Furthermore, each session with a participant lasted for about 45–60 minutes.

3.2 Testing procedure and instructions

Hostetler investigated 300 security incidents to identify cyber attacks [41]. The report identifies human error as the leading cause of incidents (37%), followed by phishing attacks and malware downloads (25%), external theft (22%), and employee theft (16%). A report claims that many costly cyber attacks could be prevented with better people-management protocols [42] including training, awareness, self-phishing simulations, and utilizing effective security utilities. Most successful cyber attacks are those in which external attackers target individuals and prey on their weakness with the goal of luring them to expose private information or act maliciously on behalf of the adversaries. A simple and easy avenue for launching such attacks is through phishing and social engineering attacks. Phishing is still considered to be a very effective means for launching cyber attacks [43, 44]. Reports show that around 91% of all cyber attacks start with some kind of phishing through emails and social engineering manipulation. The primary reason is the relative ease of social engineering attempts and phishing emails to obtain sensitive information. Given the prevalence of and risks associated with cyber-attacks, Internet users must be aware of when they are being attacked and be informed effectively.

As a result, for this study, we created sounds for phishing, malvertising, and form filling incidents to simulate scenarios where certain threats were injected.

3.2.1 Metrics for formative evaluation

The formative evaluation presented in the paper reports both qualitative and quantitative data across the two testing phases *Out of context* and *in context*. More specifically, the criteria for evaluation of the sonification approach described in the paper consists of following:

1. Correct identification and remembrance of sounds and their intentions: This metric measures whether the participants were able to correctly identify what the sonification conveys and the associated security threat.
2. Average pleasantness and urgency caused by listening to each sound: This measures the participants responses of sonification in terms of how pleasant the sound is and whether or not it draws participant's attention measured of a likert-scale.
3. Best sound rating: This measure was included to gauge if there emerged any patterns among the participants when associating a sonification that best fits a security threat. The formative evaluation aims to test natural sounds that the users can remember easily without requiring any significant training.
4. Heard the alert: It is essential to measure if the participants heard the alert when a security threat arises. This is useful to measure if the sonifications chosen can grab participant's attention while performing tasks.

The two phases are described in detail in the following sections.

3.2.2 The three stages of "Out of Context" formative evaluation

During the evaluation, a research assistant read the description of three security threats as described in Table 1 for each participant. There were no distractors in this study and the research assistant read the description of the three focused threats for the participants (i.e., Phishing, Malware Downloading, and Form-Filling). The participants were instructed that they could ask to repeat the descriptions as many times as they would like if the descriptions were unclear to them. The evaluation was divided into three stages:

Stage 1. *Measuring Identifiability, Pleasantness, and Urgency*. In this stage, each participant was asked to rate nine sounds produced for our previous study

Table 1 The final set of sonifications and brief explanations for why those sounds were chosen

Attack	Sonification and Brief Rationales
Phishing	(1) Sonification. Casting a Fishing Reel <i>Rationale.</i> Users should recognize it as a fishing reel and then connect that with a phishing attack.
	(2) Sonification. Breaking Glass <i>Rationale.</i> Phishing attacks often involve attempts to steal information, which is somewhat analogous to a burglary, and it was thought that this sound would have a negative connotation.
	(3) Sonification. Opening a Rusty Door <i>Rationale.</i> Phishing attacks often involve attempts to steal information, which is somewhat analogous to a burglary, and thus, this sound would suggest such a negative connotation.
Malware Downloading	(1) Sonification. Dropping a Bomb <i>Rationale.</i> Malware downloading can wreak havoc on one's computer system, and it was thought that this sound would have a negative connotation.
	(2) Sonification. Pouring Water into a Container <i>Rationale.</i> Water filling the container was thought to be analogous to the process of downloading a file.
	(3) Sonification. Siren Sound <i>Rationale.</i> Malware downloading can wreak havoc on one's computer system, and it was thought that this sound would have an urgent connotation.
Form-Filling	(1) Sonification. Typing on a Keyboard <i>Rationale.</i> Typing on a keyboard is often a component of filling out an online form.
	(2) Sonification. Bubbling Water <i>Rationale.</i> The bubbling was thought to be analogous to an ongoing process such as filling out a form.
	(3) Sonification. Playing a Slot Machine <i>Rationale.</i> The threat during form-filling is exposing sensitive information, which often involves money.

[12, 13]. Each of the three security threats had three sonifications associated with it. Thus, there were a total of nine sounds. The order of playing each sound was randomized for each participant to avoid possible biases. After playing each sound, the participants were first asked to describe what security situation the sound conveyed (i.e., Identifiability) out of the three threat descriptions that were read to them earlier. Then, they were asked to rate each sound based on the Pleasantness, and Urgency of each sound. More specifically:

- **Identifiability** Participants were asked to select the cyber-threat that they thought the sonification was meant to convey
- **Pleasantness** Participants were asked to rate each sound based on its pleasantness on a 5-point Likert scale – with 1 being 'extremely unpleasant' and 5 being 'extremely pleasant.'
- **Urgency** Participants were asked to rate each sound based on how urgent the sound was to them in terms of a 5-point Likert scale – with 1 being 'I would definitely ignore it', and 5 being 'I would definitely react to it.'

According to the sonification handbook [45], a sound designer needs to carefully make decisions about what

approach to sonification works best for a system. For example, a pleasant sound may be easier to recognize but it may not be effective in conveying the intended meaning. Therefore, factors such as sound's pleasantness, urgency may play important characteristics while designing sonifications for cyber security threats. Additionally, choosing sounds familiar to the users reduce training time and thus chances of error [46].

The responses were then recorded for each of the nine sounds. If participants were unable to identify the correct security threat pertaining to each sound, they were informed about the correct option.

Stage2 Selecting the Best Sonification for Each Security Threat. In this stage, participants were asked to select each sound that they thought best conveyed the intended security threat. The participants selected one sound from each security set with three sounds produced for each. The order in which the sonification was presented was also randomized to avoid biases. In addition, we also asked the participants to briefly explain the rationale behind their choice for each threat.

Stage3 Measuring Memorability. In the final stage, participants re-listened to the sonifications in random order and then were asked to recall what security situation each sound was supposed to convey. The key idea was

to see if the participants would be able to recall the intended meaning of sonification after just one exposure to the sound without any guidance. Measuring memorability after just one exposure would help to understand whether the use of natural sounds would help participants remember the associated threat. It is important to note that we did not study the effect of the repeated exposure to sounds in memorability.

3.2.3 The “In Context” formative evaluation

For the in context formative evaluation, the participants used the *CyberWarner*, a Google Chrome extension that the research team developed for the purpose of this study (see Sect. 4 for details). We considered four different scenarios to sonify each of the threats described in Table 1. This evaluation required participants to work with real Websites. For example, in the case of Phishing, we chose to sonify two different aspects of phishing - namely visiting a Website with an invalid certificate and the other one being a Website whose URL would suggest that users should suspect a phishing attack.

The three sonifications chosen were 1) *casting a fishing reel*, 2) *sounding a siren*, and 3) *typing on a keyboard*. The scenarios were developed in such a way that two of them would generate a sound alert, i.e., task-relevant, while one of them would not, i.e., non-task relevant. A task is defined as an activity that the participant were asked to perform while visiting each Website (e.g., registration on the Website).

The order of the application domain and the scenarios was randomized so that the participant would not know which task would generate a certain sound alert. Additionally, by randomizing the order, we aimed to ensure that effects such as learning and fatigue could not confound the tasks (e.g., tasks at the beginning being privileged with low fatigue vs. tasks at the end being hindered by fatigue). Moreover, the evaluation presented in this work is concerned with exploring whether the participants were able to remember what the sonifications conveyed rather than an individual's remembering ability. The descriptions of these scenarios are given in Tables 2 and 3.

For each of the scenarios, we asked participants as before - to explain their rationale behind their choices and what action they would have taken in response to the sound if they were not told to stop after hearing the alert. This was important so that we could analyze whether the participants would take the necessary actions in response to the threats.

4 CyberWarner: a sonification sandbox for alarming threats

To enable easy replications of the experiments conducted and reported in this work, the research team developed a sonification sandbox for alarming cyber threats and cues, called *CyberWarner*. The current version of the sandbox primarily sonifies threats related to downloading, various forms of Website phishing and spoofing, and form filling. The tool is developed using the Google Chrome Extension¹. *CyberWarner* uses heuristics derived from the existing literature to warn users using sounds in the event of security threats. It is different from other extensions or plugins as it functions at the “*browser level*” rather than being application-dependent or content-dependent such as in the case of Page Monitor [47], Gmail Audio Alerts [48], Wachete [49], Notification Sound [50], and Noise [51]. It is important to note that these sonifications would be played only when a security threat is detected, and thus, we do not expect them to be overwhelming because they should only occur periodically.

4.1 Google chrome extensions: a review

Google Chrome Extensions offers a whole gamut of features to extend the functionality of the Google Chrome browser. Extensions enable everything from changing the look and feel of the browser to providing additional functionality in the browser to aid day-to-day tasks [52, 53]. Chrome provides security by running each component of the extension in a sandboxed environment, which ensures each process runs in an isolated environment and can have access to only those APIs that are explicitly mentioned in the manifest file of the extension code [54, 55]. Essentially, Google extensions are made up of two components [56]:

- (1) *User-Interface Components*. These components are simple HTML and CSS (Cascading Style Sheets) features that are responsible for managing the look and feel of the extension.
- (2) *Scripting Components*. These components can be further divided into two parts:
 - (a) *Background Event Pages*: It is the heart of any chrome extension, where the main core logic of the extension resides. Background pages can be either *persistent* or *event-based*. A *persistent* page requires the background page to keep running during the entire time

¹ The sonification sandbox can be downloaded through the following link: <https://github.com/asiamina/CyberWarner>

Table 2 The scenarios used in the study (Part 1)

Threat, Scenarios, and Tasks

Threat: Phishing**Task 1. Finding Top Job Positions Available.**

1. Visit www.nsa.gov
2. Click the link on the top that reads "Career & Programs." Then, find the link where it says "IntelligenceCareers.gov/NSA" and then click "Careers" on the following page.
3. Copy and paste the first 3 job categories listed on the page in the notepad file.

Task 2. Finding Resources for Educating People about Security.

1. Visit www.nsa.gov
2. Click "Resources For" link on the top and then select Educators → Centers of Academic Excellence in cyber security → Cyber Defense.
3. In the next page, click the link that says: "For a current list of NSA/DHS CAE institutions."

Task 3. Finding Information about NSA's CSFC Program.

1. Visit www.nsa.gov
2. Click "Resources For ..." link on the top and then select Educators → Commercial Solutions for Classified Program.
3. On the next page, scroll down and find the link that says, "Click here to go to the CNSS Website." and then click it.

Threat: Form Filling**Task 1. Searching for Favorite Music Video.**

1. Visit www.youtube.com and search for your favorite music video in the search box.

Task 2. Change Account Information.

1. Open www.gmail.com
2. On the sign in page, enter udemo57@gmail.com as the email address and click Next.
3. Enter password exactly as following "dummpassword", without quotes.
4. In the top right, click "Settings."
5. Click the Accounts and Import Tab.
6. In the "Send mail as" section, click "edit info". Add the name you want to show when you send messages. At the bottom, click Save Changes.

Task 3. Findings video with maximum no. of views.

1. Visit www.youtube.com
2. Click Sign in button.
3. On the sign in page, enter udemo57@gmail.com as the email address and click Next.
4. Enter password exactly as following "dummpassword" (without quotes).
5. On the left hand side, click "Favorite" under Playlist tab.
6. Based on the list of videos on your list, find the one that has the maximum number of views. By visiting each video one by one. Note down the video title in the notepad.

the extension is up and running while an *event* page is triggered when a certain action(s) occurs and after performing its designated action it returns the control to the dormant state. Unless it is required to run the extension logic on all the pages, at all times, it is recommended that developers refrain from using the background pages as it may affect the load time of a page in the browser. Background pages have complete and full access to standard JavaScript libraries and also chrome extension APIs.

- (b) *Content Scripts:* These scripts are used when the extension needs to interact with certain Web pages in the browser. It works by injecting a specific code (e.g., JavaScript) to the source code of the page to enforce the intended action when the page is loaded. These scripts are primarily used for "message passing"

or interacting with the background page. Content scripts are designed to run with the least-privilege mechanism to ensure security [54]. They have complete access to the page's DOM (Document Object Model) objects but limited access to Google Chrome APIs [57]. Google Chrome APIs consists of libraries of functions that an extension can use to modify the different aspect of Web pages such as downloads and open tabs [58]. Document Object Models or DOMs are a tree-like hierarchical representation of all Web pages in the browser. Developers can use this hierarchical structure to manipulate the HTML dynamically by adding or removing elements from a Web page or changing certain properties of the visual elements on the Web page, e.g., background colors. If it is required by the extension to use the chrome

Table 3 The scenarios used in the study (Part 2)

Threat, Scenarios, and Tasks

Threat: File Downloading**Task 1. Looking for a List**

1. Choose a Journal of your choice and open it in your browser.
2. Copy and paste the list of most read papers on the main page in the notepad file.

Task 2. Downloading a Research Paper

1. Open a new tab and enter the URL of your favorite journal.
2. Search for a topic of your journal in the search box.
3. Download the paper of your choice by right clicking and selecting "Save Link as.."

Task 3. Downloading a Citation of a Paper

1. Open a new tab and visit <http://journals.sagepub.com/home/hfs>
2. In the Search Box, search for the following research paper by Frank A. Drews: "Human factors in critical care medical environment"
3. Click on the link to the paper in the search results.
4. In the box on the right side, click Cite and then Download Citation

Threat: Phishing Using URL Heuristics**Task 1. Looking for News**

1. In a new tab, type in eng.customs.ru and press enter.
2. Copy and paste the Top 3 News headlines in the notepadfile.

Task 2. Looking for Personal Names

1. In a new tab, type in eng.customs.ru and press enter
2. In the ABOUT section, click on the link that says Management.
3. Copy and paste the names of the first two people on the list in the notepad file.

Task 3. Looking for Individual Customs Declaration

1. In a new tab, type in eng.customs.ru and press enter.
2. Scroll down to the FOR INDIVIDUALS section on the left, click on the link that says: "Passenger customs declaration."
3. Click the first link that says: "Procedure of filling in the passenger customs declaration" and note down the date in the notepad file.

APIs (i.e., chrome.* API), the content script interacts with the background page through message passing and the background page can then use the requested API(s).

4.2 The security sonification integrated in the sandbox

The current version of CyberWarner, the sonification sandbox, implements three types of security threats and cues: (1) various forms of phishing attacks through Web browsers, (2) file downloading, and (3) form filling.

4.2.1 Security threat/cue: potential phishing attacks

There are many variations of how phishing attacks can take place. CyberWarner implements the sonification of two forms of phishing attacks: (1) visiting an unsafe Web page, whose certificate is expired or is invalid, and (2) visiting a suspicious Web page, whose URL's pattern is inspected to determine and detect a potential phishing Website:

- (1) *Invalid/Expired Secure Socket Layer (SSL) Certificate.* Secure Socket Layer (SSL) protocol is designed to ensure secure and confidential communication on the Internet. When a user requests a Web page, it is the responsibility of the browser to verify the Web page's identity by checking its SSL certificate. SSL certificates are usually signed by a trusted third party called the *Certification Authority* (CA). The signed certificates are matched with the details advertised by the Web page. In the case of a mismatch, the user is given a warning as shown in Fig. 1, alarming that the connection to the Website may not be safe. Although in theory, this warning should be sufficient in alarming the users to refrain from visiting the unsafe Website. However, as shown by many studies, most users decide not to heed the warning and proceed to the subsequent page anyway, making them vulnerable to phishing attacks [17, 59, 60]. The sonification sandbox incorporates a sonification for this facet of phishing attacks to further alarm users, in addition to visual alarming and let them be aware of potential phishing attacks.

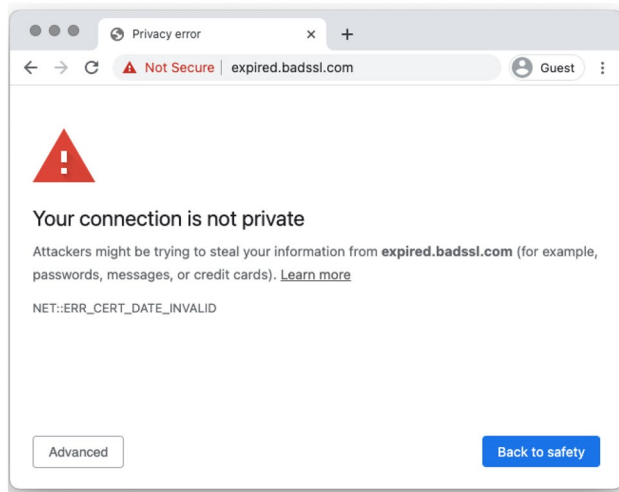


Fig. 1 An invalid certificate warning in Google Chrome



Fig. 2 Structure of a typical URL address

- (2) *URL Patterns and Heuristics*. URL heuristics are used to determine whether a URL address is likely to be a phishing Website. Many heuristic techniques involve the use of complex machine learning or data mining algorithms to estimate if a Website is likely to be a phishing Website. A typical URL structure is made of (1) protocol, (2) sub-domain, (3) primary domain, and (4) top-level domain (TLD) followed by an optional path domain. An example of a typical URL is shown in Fig. 2.

Given that we wanted to limit our scope to heuristics that could be programmed using JavaScript and would give the desired results, CyberWarner implemented the following heuristics based on our literature review of URL heuristics [61–68]:

- (i). *Number of Dots in the Domain* When the number of dots in a domain exceeds a certain threshold, then the URL is probably suspicious. Based on our experimentation and study, we decided to keep the threshold in CyberWarner, i.e., the number of dots in the path, as 5. A study reports that the number of dots in a suspicious URL is usually more than 4 [69]. To reduce the number of false positives, we

consider the number of dots allowed in the given URL to be 5.

- (ii). *Length of the URL* URL length of more than 75 characters is considered to be suspicious. According to a study, normal length of the URL should not exceed 54 characters [61]. In order to reduce the number of possible false positives, we consider 75 characters. Nevertheless, this value can be changed while installing CyberWarner.
- (iii). *Suspicious Characters* The presence of symbols like "@" or "\" is another indicator that the URL might be suspicious.
- (iv). *Presence of an IP Address* Unless a user is accessing any Intranet Website, the presence of an IP address in the URL is an indicator of the Website being malicious.
- (v). *Known Malicious TLDs* Some phishing Websites are known to use certain *top-level domains* (TLD) that make them labeled as being a phishing Website (e.g., a URL with .bz domain). CyberWarner incorporates 18 most common malicious TLD's compiled from various sources.
- (vi). *No Use of HTTPS* Although the use of the HTTPS protocol is not mandatory in many legitimate Websites, almost all phishing Websites use only simple HTTP. Therefore, the use of simple HTTP is one of the heuristics to mark a URL as suspicious.

In CyberWarner, each of these URL heuristics was assigned a certain weight. Every visited URL is analyzed using these heuristics in real-time. If there is a match between certain characteristics of the URL and the heuristics, its corresponding weight w_i is added to a summation variable W .

When the value of the count variable W exceeds a certain *threshold* (θ), we estimate that URL to be suspicious and thus play the corresponding sound alert to the end-user. After some experimentation and preliminary testing, we kept an overall *threshold* θ value as 4. The choice of 4 was based on our review of the existing literature on URL heuristics with their focus on utilizing quantitative measures to identify phishing Websites.

We also inspected several malicious URL's from www.phishtank.com to have some insights regarding this threshold value. The weight assigned for each of these heuristics in our extension is shown in Table 4. A similar approach for measuring the weights of heuristic features and their contributions to the overall prediction of spamicity of a given URL is presented by Jo et al. [63] where a simple logistic regression is used to predict the spamicity of URLs. Here, we did not perform any regression analysis. Instead, we performed some pilot studies and adjusted the weights accordingly. As an example, a malicious URL using only http [weight + 1] and a

Table 4 URL Heuristics and their assigned weight

	URL Heuristic	Assigned Weight(W_i)
1	Number of Dots in Domain	1
2	Length of URL ≥ 75	1
3	Suspicious Characters '@', '\'	3
4	Presence of IP address	3
5	Known malicious TLD	2
6	Using only HTTP	1

The summation variable **W** can be represented mathematically in the form of following equation:

$$W = \sum_{i=1}^6 w_i \quad (1)$$

where, $i = 1, 2, \dots, 6$ is the URL heuristic.

Thus, **If:** $W \geq \theta$; URL is malicious

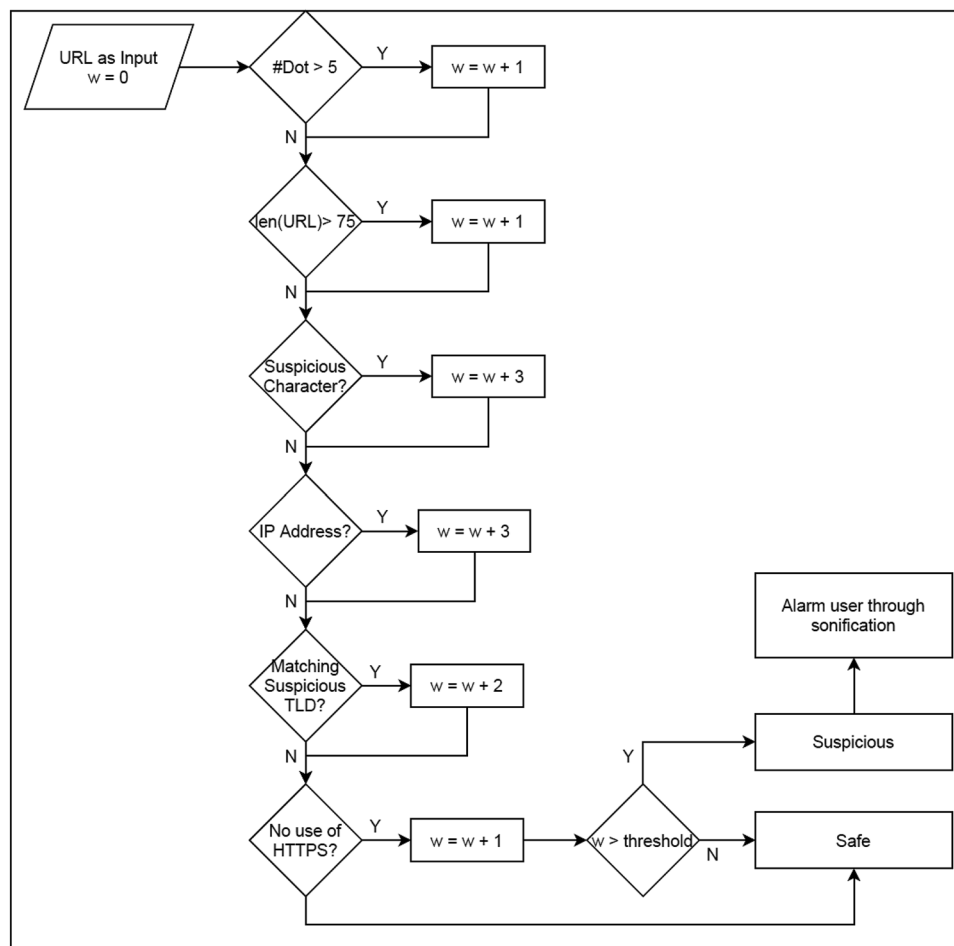
Else: URL is safe

This process is illustrated in the form of a flowchart as depicted in Fig. 3.

malicious Top-level-domain (TLD) such as “.bz” [weight + 2] and length of URL [weight + 1] would add up to a total weight of 4. Note that the URL may contain more URL heuristics that could help to identify it as a malicious domain. However, once it exceeds the threshold, it indicates the presence of a malicious URL. Based on the pilot study, we increased the value to 4 from the initial value of 3 in order to reduce false positives and thus have a more sensitive value for identifying a malicious URL.

4.2.2 Security threat/cue: form-filling

It is often observed that some users are not very careful about their surroundings when they are entering their credentials (e.g., password) or sensitive information (e.g., credit card number) in a Web form. Although when a user enters their password in a form field, a series of dots or asterisks are displayed on-the-screen. There is, however, no guarantee that someone standing in the near vicinity of the user is not paying attention to the keys that the user is

Fig. 3 URL-based heuristics

typing on the keyboard. This situation is most likely to be observed on shared computers or while using a computer system in a public place, e.g., a library. The sandbox implements a sound alert for such situations. When users are about to type in their passwords or sensitive information, CyberWarner would alert them by playing a sound so that they can be more careful of their environment and thus to keep their passwords protected from prying eyes.

4.2.3 Security threat/cue: file downloading

Malicious software encompasses programs that have the potential to harm a computer system, a user, or the network. Despite the widespread use of anti-virus software, malware still manages to be installed on the local host computers through downloads. While malware detection on the fly is not only challenging but difficult to hard code in the Chrome extension, we tried to create a sound alert to notify the user that they may be downloading a potentially dangerous file and thus proceed with caution while handling it. Although the most common malware that can be found are executable files, there are several other file formats such as *.doc and *.pdf files that can contain malware. These types of files are known to carry malicious code through virus or malicious code (e.g., Java scripts) that can be integrated into these portable files. The current version of CyberWarner alarms users whenever there is a downloading activity. In practice, not all downloaded files are malicious. A feature that can be added to CyberWarner is to integrate it with some anti-virus software to make sure that only malicious files are causing the alarm sounds to be played.

5 Analysis and results

5.1 Results for the “Out of Context” formative evaluation

The result of the out of context formative evaluation is depicted in Fig. 4 and Table 5. It is apparent from Fig. 4 that the participants preferred sounds that were semantically close to the security threat. For instance, 58% of the participants rated “casting a fishing reel” sonification as the best to represent phishing, while 89% of the participant rated “typing on a keyboard” as the best sonification for representing the form-filling cue. In the case of malware downloading, 50% of the participants rated “sounding a siren” as the best representation followed closely by “dropping a bomb” by 46%.

The results are generally consistent with our earlier formative evaluation with users who were visually

Table 5 Results of “out-of-context” study for participants who were not visually impaired

Sonification	%Correctly		%Rated
	Identified	Remembered	Best
<i>Phishing</i>			
Casting a fishing reel	46	73	58
Breaking glass	31	69	23
Opening a rusty door	31	69	19
<i>Malware downloading</i>			
Dropping a bomb	81	88	46
Sounding a siren	39	77	50
Pouring water	35	58	4
<i>Form-filling</i>			
Typing on a keyboard	92	96	89
Bubbling water	12	54	4
Playing a slot machine	27	62	8

impaired. Sounding a siren was rated as the best sound in both cases. However, dropping a bomb stood close to sounding a siren compared to participants who were visually impaired, who rated dropping a bomb sound (1 out of 5 participants) and sounding a siren (4 out of 5) respectively.

Figures 5 and 6 illustrate the normalized z-scores and unnormalized likert scores for pleasantness and urgency, respectively. As illustrated in Fig. 5b, the pleasantness z-score values for sonification of fishing rod, breaking glass, and rusty doors are mostly in the range of $[-1.5, +0.5]$ standard deviation of the mean; whereas, as shown in Fig. and 5d, the pleasantness z-scores of the sonification for dropping a bomb, siren, and pouring water are in the range of $[-1.5, +1.5]$ standard deviation of the mean. Moreover, as shown in Fig. 5f, the pleasantness scores of sonification for typing on a keyboard, boiling water, and slot machine are in the range of $[-1.00, +2.00]$ standard deviations above the mean indicating that these sounds are considered more pleasant than the sounds designed for sonification of those shown in Figs. 5b, d.

Similarly, Fig. 6a illustrates the urgency z-scores for phishing sonification (i.e., fishing rod, breaking glass, and rusty door). The urgency z-score computed for the breaking glass sonification is roughly 1.5 standard deviations above the mean compared to fishing rod and rusty door sounds, indicating that breaking glass draws participants' attention more than the other two sounds. Figure 6c, shows the urgency z-scores for sonification of malware download. As observed in figure, the urgency of dropping a bomb and the siren sounds are higher compared to pouring water sound. This means that the urgency ratings is higher (draws more attention) for the first two sounds compared to the pouring water sound. Finally, in Fig. 6e

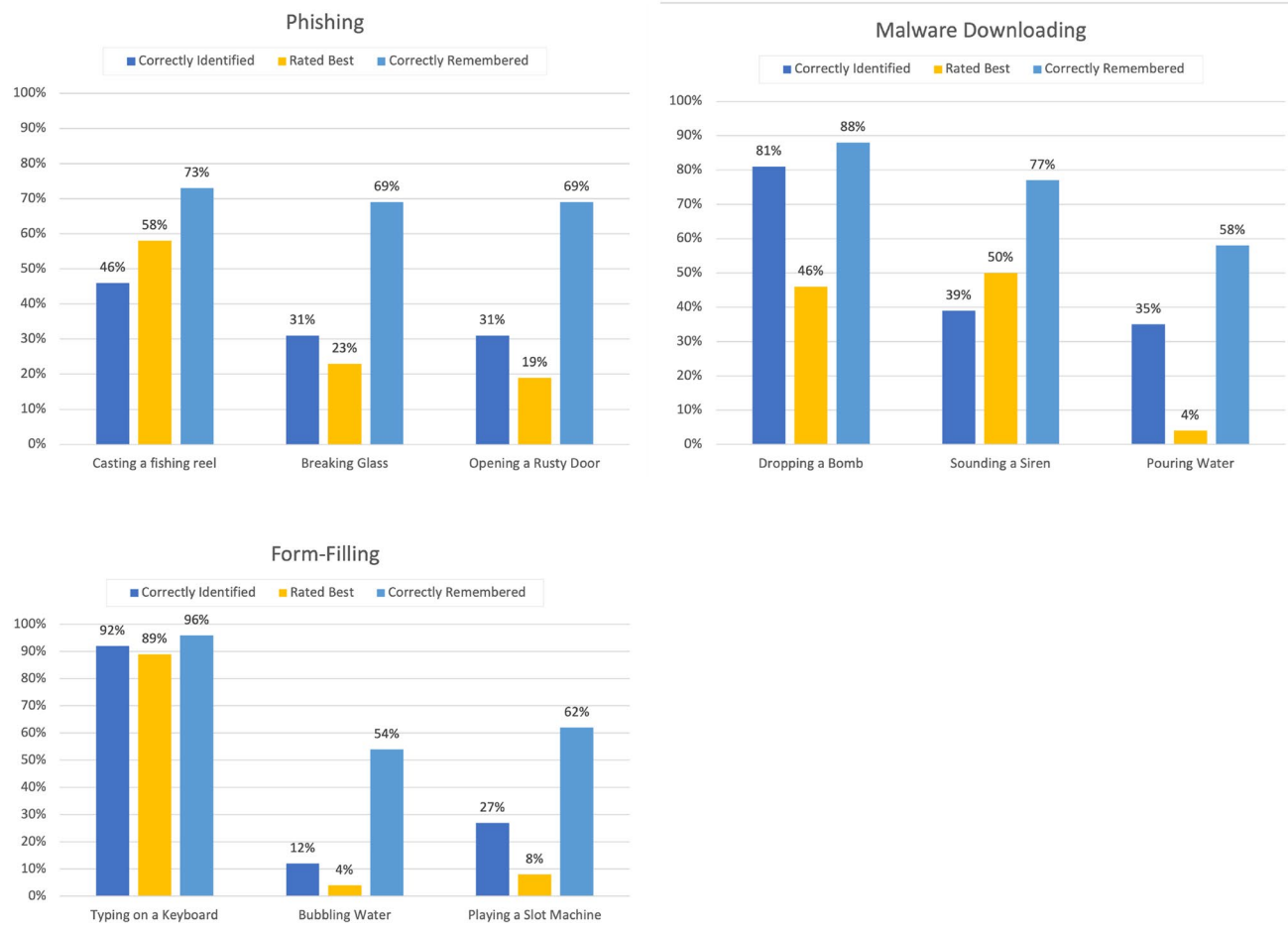


Fig. 4 The Out-of-Context formative evaluation for users who are not visually impaired

all of the three sounds designed for form-filling sonification have a z-score rating of around 2 standard deviations below the mean indicating that these sounds were not considered as urgent by the participants in drawing their attention.

5.2 Results for the “In Context” study

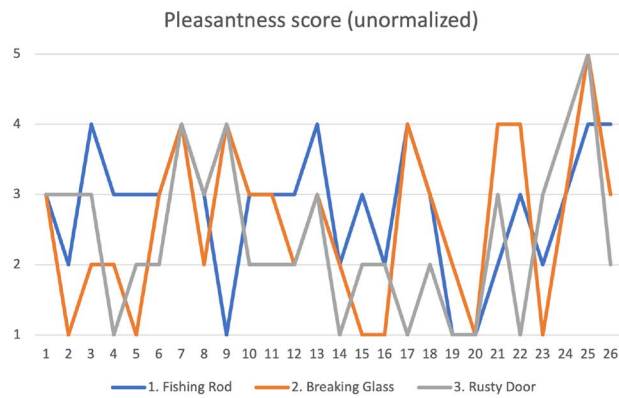
According to Fig. 7 (Table 6), in all cases, the participants heard the alerts when navigating the target Website. The percentage of participants who correctly identified each threat was between 73% and 100%. The percentages are somewhat greater than those captured for users who are visually impaired from our previous study. This is because, unlike the case for the visually impaired, we did not use any distractors in the study performed with participants who were not visually impaired. In other words, there is only a 33% chance that the participants would randomly guess the correct threat. We believe this number is sufficiently low. Adding distractors would further reduce the probability and also risk the study running too long.

The other evaluation criteria measured for users who are visually impaired (i.e., task-relevant and non-task relevant) were not applicable for users without visual impairment, as users without visual impairment use the mouse for navigation through the form and do not typically use the keyboard and in particular, the TAB button to navigate a form (i.e., the TAB button is usually used by users who are visually impaired to navigate a form field by field; whereas, the TAB button is the most important button for users who are visually impaired for navigation purposes).

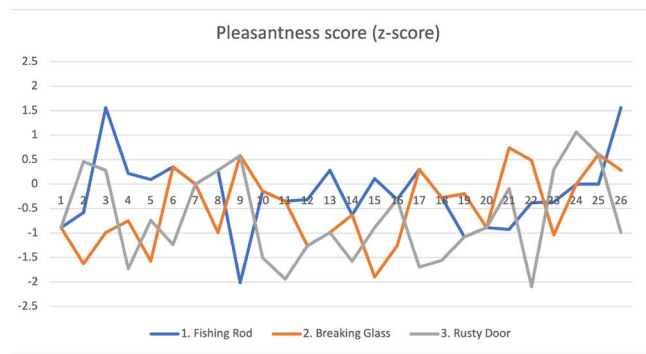
5.3 Discussion

5.3.1 Participants responses/comments

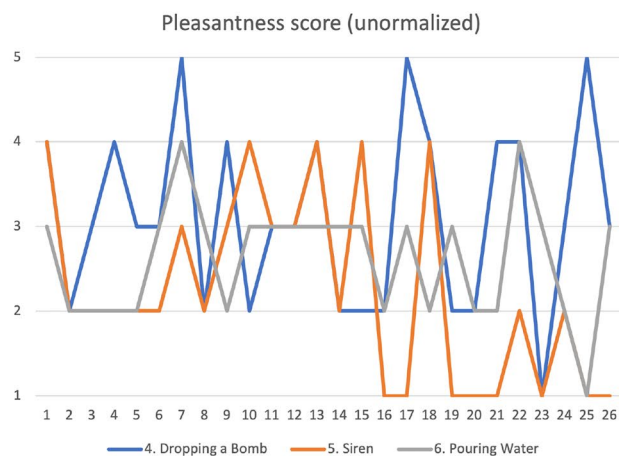
Table 7 shows some of the responses from the *in-context* study with sighted participants about what they would have done if not told to stop upon hearing the sound. The study described in this paper is not only to evaluate the sonifications but also to gauge if the participants would



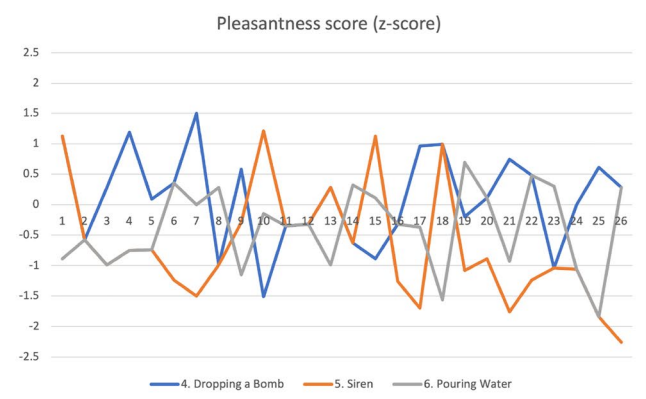
(a) Phishing (Likert Scores)



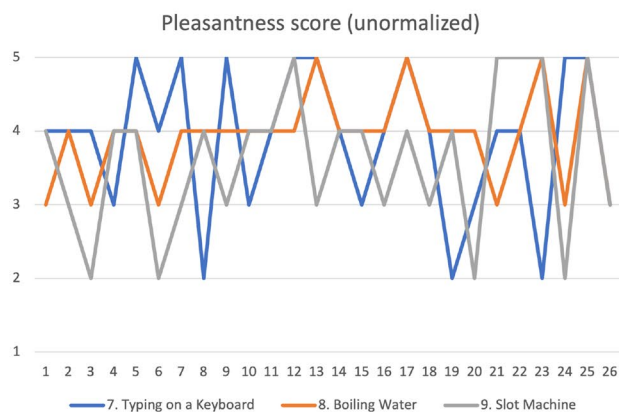
(b) Phishing (Z-Scores)



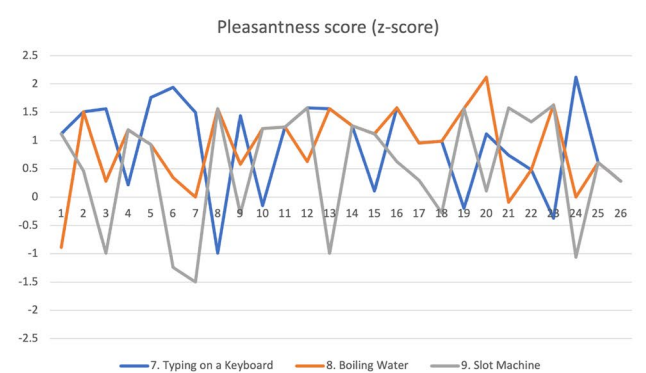
(c) Malware Downloading (Likert Scores)



(d) Malware Downloading (Z-Scores)

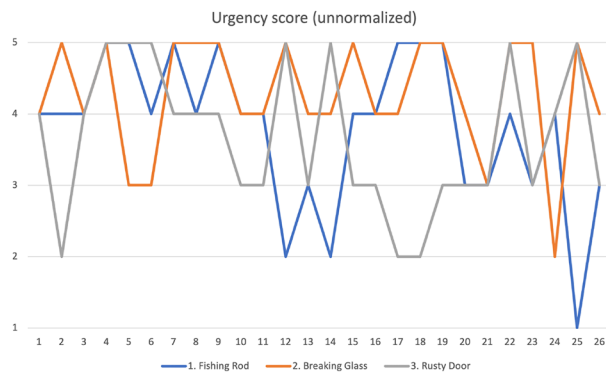


(e) Form Filling (Likert Scores)

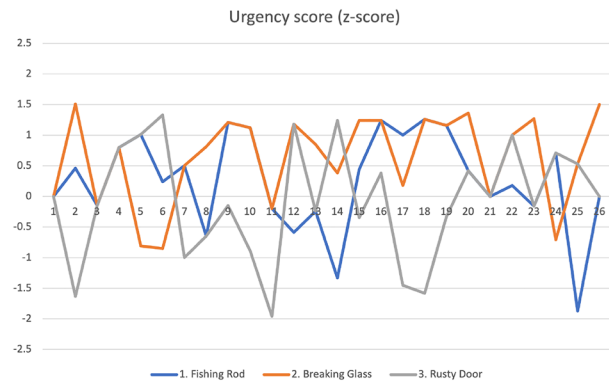


(f) Form Filling (Z-Scores)

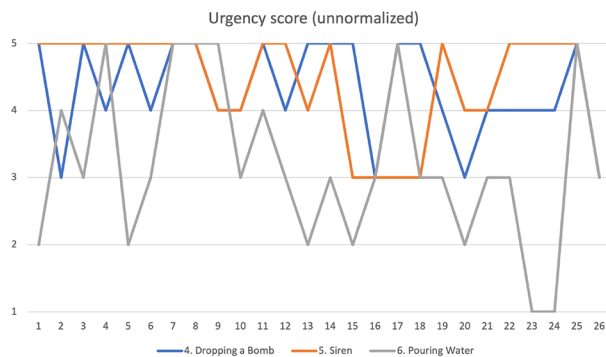
Fig. 5 The Unnormalized and Normalized scores for Pleasantness rating



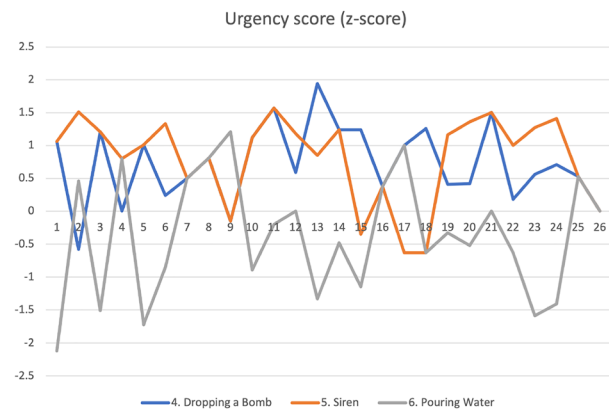
(a) Phishing (Likert Scores)



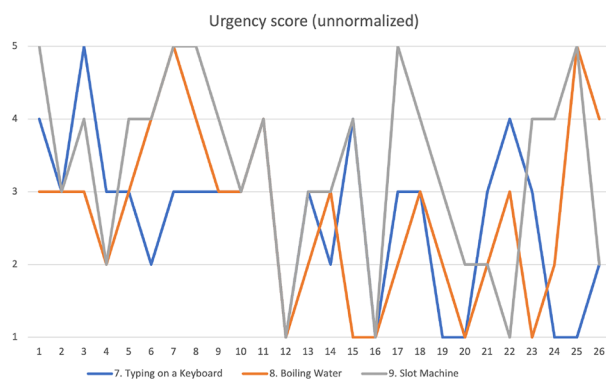
(b) Phishing (Z-Scores)



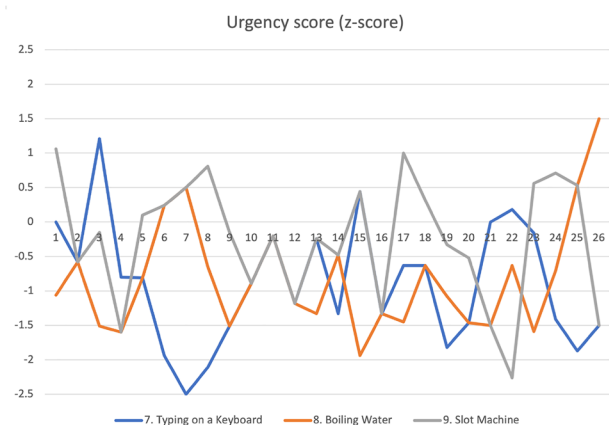
(c) Malware Downloading (Likert Scores)



(d) Malware Downloading (Z-Scores)



(e) Form Filling (Likert Scores)

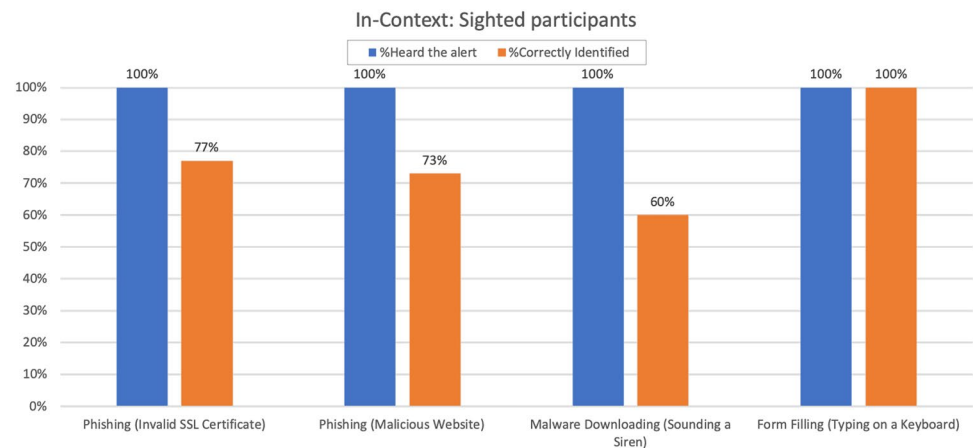


(f) Form Filling (Z-Scores)

Fig. 6 The Unnormalized and Normalized scores for Urgency rating

Table 6 Results of “in-context” study for participants who were not visually impaired

The aspect sonified	Sonification	Alert % heard the	the Threat identified % correctly
<i>Phishing</i>			
Invalid SSL Certificate	Casting a fishing reel	100	77
Malicious website		100	73
<i>Malware</i>			
Potentially dangerous files based on the file extension (e.g. .exe, .swf etc.)	Sounding a Siren	100	92
<i>Form-filling</i>			
Password input field on Web forms	Typing on a keyboard	100	100

Fig. 7 The In-Context study for sighted participants**Table 7** Participants responses for the “In-context Study”

Cyber-threat	Participants comments	Correctly Identified Threat?
Phishing (Invalid Web page Certificate)	- Go back and see if what I did caused the sound and look further into that	Y
	- Would've Exited my browser	Y
	- Looked it up on my phone what the sound meant	Y
	- I was going on a non-secure Website, I would have stopped	N
	- Because I was trying to go to another site and my information wasn't private, I would've clicked "go back to safety" button when it popped up	N
Phishing (URL Heuristics)	- I would be concerned and stop and figure out what happened. Maybe go back and click on link again	Y
	- Would've double-checked the Website to see if I was mislead somewhere else	Y
	- Would have just clicked on one of the people because it is a federal service Website	N
	- Would've closed the page. Thought something is wrong with the Website	N
Form-Filling	- Would have stopped typing	Y
	- Would be more aware of who was around me	Y
	- Continued signing in	Y
	- Probably would've continued. No elaboration what's wrong - just the noise	Y
Malware Downloading	- Closed all my tabs and turn off pop-ups and not download the file again	Y
	- It downloaded something, may have some code in it. Probably would've deleted the file immediately	Y
	- I would still download since it is just a citation but try to figure out what went wrong	Y
	- I would've stopped this step. Noise grabs attention	N

stop their tasks if they heard the sounds during the simulated scenarios.

For the phishing (invalid certificate) scenario, the participants exhibited a rational choice of exiting or closing the browser window even if they were not able to identify the phishing threat through the sonification.

For the form-filling scenario, all the participants were able to correctly identify what the sonification (typing keyboard sound) conveyed and indicated that they would have been more careful of their surroundings when entering their passwords in the Web page.

Similarly, the participants denoted that they would delete or cancel the file for the malware downloading scenario. These responses indicate that even though the participants did not always remember what threat the sonification conveyed, the participants stipulated a rational action in response to the sound in real-world situations.

It should be noted that as we did not use actual malware and phishing Websites out of the security concerns of the participants and to avoid any unpredictability during the formative evaluation. As a result, a few of the participants stated that they would have ignored the sonification warning or would have preferred a textual warning in addition to the sonification, to comprehend the situation and make an informed decision. For example, in phishing (URL heuristic) scenario, one of the participants pointed out that the Website appeared to be a legitimate federal Website and as a result, the participant would have continued browsing the Website despite the sonification warning:

"(I) would have just clicked on one of the people because it is a federal service Website."

5.3.2 Comparison: participants who were not vs. were visually impaired

In Sect. 3, we listed several motivational questions regarding the usefulness and formative evaluation of the sonifications for general Internet users. To reiterate, our previous work [12, 13] contained 5 participants who were visually impaired whereas the current work presented in the paper reports the results with 26 participants who are not visually impaired (sighted participants).

Both groups of participants agreed on rating (i.e., Rated Best) the sounds created for phishing, malware downloading, and form-filling as casting a fishing reel, sounding a siren, and typing on a keyboard respectively. However, in the case of the sighted participants, sounding the siren (rated best 50%) came marginally close to dropping a bomb (rated best 46%) as compared to sounding the siren (rated best 80%) and dropping a bomb (rated best 20%) in case of visually impaired participants. Both groups

of participants agreed on the pleasantness levels of the sounds (i.e., Average Pleasantness) that were created for the sonifications. There are some slight variations such as the pleasantness of "pouring water" increasing from 52.4% to 64% for participants without and with visual impairment respectively. Both groups of participants agreed on the urgency level of the sounds (i.e., Average Urgency). Specifically, both groups agreed that Breaking Glass, Sounding a Siren, and Playing a Slot Machine, convey the most urgency.

Some differences were observed when participants were asked whether they remembered the sonification. The number of participants with visual impairment who remembered the sonification correctly was greater than those without visual impairment. This is an interesting observation implying that individuals who are visually impaired tend to remember events and corresponding sounds that occurred in the surrounding environment better than those without visual impairment. There are a couple of exceptions where participants without visual impairments remembered the sounds correctly (i.e., "bubbling water" and "playing a slot machine"; 80% of participants who were not visually impaired remembered the meaning of those sonifications correctly).

There is a complete consistency between the two groups of participants in hearing the alarms while navigating the Web applications and Websites. On the other hand, there are some variations to correctly identifying the threats. The differences might be because of the Web applications that were used for participants who are visually impaired were fake and created by our research team; whereas, the Websites that we used for the formative evaluation for visually sighted participants were real enabled with CyberWarner installed on their browsers. Intuitively, if participants are given a superficial and fake Web application to navigate they would expect some strange or unexpected issues. However, a key takeaway lesson is that the sonifications were able to catch the participants' attention regardless of whether they were visually impaired or not. Thus, it seems that the sonification is effective and informative regarding informing the users about imminent threats.

6 Conclusion and future work

This research explored whether sonified cyber security threat indicators could be used to effectively warn users without visual impairments about cyber security attacks. The results of the formative evaluation conducted were promising. Specifically, the results suggested that it is possible to develop sonified cyber security threat indicators that users intuitively understand or, more commonly, that

users can understand with minimal experience. More specifically, the current formative evaluation was conducted with participants without visual impairments in order to 1) how sonification is generally acceptable? and 2) how different users with and without visual impairments perceive the developed sonification?. We observed that both sets of participants perceived the designed sonification positively. The authors also tested the designed sonification in realistic tasks where the users were asked to navigate a real Website. We observed some changes as follows: in the case of dealing with fake Websites, users are more cautious informed about malicious activities; whereas, when navigating real Websites, they are less informed. This might be due to the appearance of the navigating Websites. Fogg et al. [40] report that people usually rely on peripheral cues, such as appearance, for assessing the credibility of Websites.

Further, qualitative results suggested ways to improve the sonifications to better represent the various cyber security threats which will guide future development. The results suggest that sonified cyber security threat indicators could be part of a solution to the problem of how to warn users about cyber security threats, and that such sonifications warrant further research. The paper also introduced CyberWarner, a sonification sandbox for cyber security that can be downloaded and installed for researchers and general Internet users. Replication is important to advance the state-of-the-art of empirically-driven observations and then transform these observations into knowledge. We developed this add-on extension to help other researchers replicate similar studies easier. CyberWarner enables sonification for Google Chrome and also it is very easy to replace the sound integrated into the tool. CyberWarner is also hosted on GitHub and thus accessible to all researchers to replicate the studies or change the sounds or use as it is in similar studies or settings.

The sonifications were found useful to draw users' attention and thereby, aid them in making an informed decision. It should be noted that sonifications are not meant to replace visual warnings but rather can be used complementary to each other. This is due to the limitations of the human anatomy as there are ten times more cortical neurons for visual processing compared to hearing and thus, sonifications may not always precise compared to visual warnings [70]. E.g., sonification can be used along with visual warnings to warn users' of a weak password during account registration [71]. Sonification can offer an additional modality to warn users of imminent cyber security threats. E.g., sonification can be useful in security operation centers (SOC) where security fatigue can arise due to a large number of alerts generated on daily basis or while the security practitioners are away from SOC [72]. While we did not explicitly ask the participants if they

would use CyberWarner on their systems, we believe the use of sonification such as the one described in the paper may augment existing security infrastructure to offer better security to the users. Future research should formally examine how a sonification's utility and usability are influenced by its pleasantness, urgency, and conspicuity. Moreover, the effectiveness of sonification after repeated or multiple exposure should be explored more formally via experimentation. The present results indicate that 73% of the participants were able to correctly identify the cyber threat after just one exposure, indicating that the use of natural sound does improve memorability. Having a better understanding of those relationships would facilitate the future development of effective sonifications.

Finally, future research should also explore ways to optimize various facets of the sonification development process. For example, the process of finding and selecting candidate sonifications was cumbersome; it would be advantageous to develop effective ways to automate, at least certain parts, of that process. It is also important to identify a representative subset of cyber threats for sonification since it is practically infeasible for end-users to remember a large number of sounds and their implications. Although the use of sonification may have unintended side effects such as an added demand on users' attention to try to remember what the sonifications convey. It should be noted that the sonifications themselves would only play in the event of cyber threats. The CyberWarner can be further fine-tuned to avoid false positives.

It is also important to note that cyber security is a socio-technical problem. Similarly, privacy concerns are socio-technical issues. Hence, while there might be some technical solutions for technical problems, there is no silver bullet approach to address the socio part of cybersecurity. In this work, we targeted English-speaking users and thus came up with a set of sonification that reflects their culture and habits for the sonification (e.g., Phishing vs. fishing). There is a need to perform similar studies for non-English speaker users, and thus different sonification may be created to reflect different perceptions and cognition influenced by cultural differences. One of the limitations of the work presented in the paper is the lack of older participants. Future work should consider replicating the evaluations with a representative sample consisting of adults from diverse age groups.

Acknowledgements Thanks to Thomas Hughes for creating and formatting the sounds. Thanks to Rona Pogrud for recruiting the participants for the first part of this study, Thanks to Theresa Nguyen, John Rose, Miriam Armstrong, and Tim Salau for conducting the formative evaluations. The authors would like to thank the participants for their insightful comments and feedback. This work is supported by National Science Foundation (NSF) under award numbers: CNS-1347521 and SES-1564293.

Author Contributions Conceptualization, Akbar Siami-Namin, Keith Jones and Rattikorn Hewett; Data curation, Prerit Datta and Keith Jones; Investigation, Akbar Siami-Namin and Keith Jones; Methodology, Akbar Siami-Namin and Keith Jones; Project administration, Akbar Siami-Namin; Software, Prerit Datta; Supervision, Akbar Siami-Namin; Writing – original draft, Akbar Siami-Namin and Keith Jones; Writing – review & editing, Akbar Siami-Namin, Prerit Datta and Keith Jones.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Corporation S (2017) Internet Security Threat Report. Tech. rep. <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>
2. Corporation S (2018) Internet Security Threat Report. Tech. rep. <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf>
3. Thales: Thales Data Threat Report. Tech. rep. (2018). <http://go.thalesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf>
4. IBM Security: IBM X-Force Threat Intelligence Index (2018). <https://www.ibm.com/security/xforce>
5. de Paula R, Ding X, Dourish P, Nies K, Pillet B, Redmiles D, Ren J, Rode J, Filho RS (2005) Two experiences designing for effective security. In: Proceedings of the 2005 Symposium on Usable Privacy and Security, SOUPS '05, pp. 25–34
6. Stanton B, Theofanos MF, Prettyman SS, Furman S (2016) Security fatigue. *IT Prof.* 18(5):26–32
7. Pham HC, Brennan L, Furnell S (2019) Information security burnout: Identification of sources and mitigating factors from security demands and resources. *J Inf Secur Appl* 46:96–107
8. Parkin S, Krol K, Becker I, Sasse MA (2016) Applying cognitive control modes to identify security fatigue hotspots. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association, Denver, CO
9. Tanimoto S, Nagai K, Hata K, Hatashima T, Sakamoto Y, Kanai A (2017) A concept proposal on modeling of security fatigue level. In: 2017 5th Intl Conf on Applied Computing and Information Technology/4th Intl Conf on Computational Science/Intelligence and Applied Informatics/2nd Intl Conf on Big Data, Cloud Computing, Data Science (ACIT-CSII-BCD), pp. 29–34
10. Furnell S, Thomson KL (2009) Recognising and addressing 'security fatigue'. *Computer Fraud & Security* 11:7–11
11. Olt C, Mesbah N (2019) Weary of watching out? - cause and effect of security fatigue. In: ECIS
12. Siami Namin A, Hewett R, Jones KS, Pogrund R (2016) Sonifying internet security threats. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, CHI EA '16, pp. 2306–2313
13. Namin AS, Jones KS, Hewett R, Pogrund R (2016) The Sounds of Cyber Threats. SOUPS 2016. <https://www.usenix.org/sites/default/files/soups16poster10-namin.pdf>
14. Acer ME, Stark E, Felt AP, Fahl S, Bhargava R, Dev B, Braithwaite M, Sleevi R, Tabriz P (2017) Where the wild warnings are: Root causes of chrome https certificate errors. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, pp. 1407–1420. ACM
15. Egelman S, Cranor LF, Hong J (2008) You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '08, pp. 1065–1074
16. Akhawe D, Felt AP (2013) Alice in warningland: A large-scale field study of browser security warning effectiveness. In: Proceedings of the 22Nd USENIX Conference on Security, SEC'13, pp. 257–272
17. Felt AP, Reeder RW, Almuhammedi H, Consolvo S (2014) Experimenting at scale with google chrome's ssl warning. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '14, pp. 2667–2670
18. Reeder RW, Felt AP, Consolvo S, Malkin N, Thompson C, Egelman S (2018) An experience sampling study of user reactions to browser warnings in the field. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18, pp. 512:1–512:13
19. Egelman S, Schechter S (2013) The importance of being earnest [in security warnings]. In: Sadeghi AR (ed) Financial Cryptography and Data Security. Springer, Berlin Heidelberg, pp 52–59
20. Sotirakopoulos A, Hawkey K, Beznosov K (2011) On the challenges in usable security lab studies: Lessons learned from replicating a study on ssl warnings. In: Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS '11, pp. 3:1–3:18
21. Anderson BB, Kirwan CB, Jenkins JL, Eargle D, Howard S, Vance A (2015) How polymorphic warnings reduce habituation in the brain: Insights from an fmri study. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15, pp. 2883–2892
22. Anderson BB, Jenkins JL, Vance A, Kirwan CB, Eargle D (2016) Your memory is working against you: How eye tracking and memory explain habituation to security warnings. *Decision Support Systems* 92, 3 – 13. A Comprehensive Perspective on Information Systems Security - Technical Advances and Behavioral Issues
23. Bravo-Lillo C, Cranor L, Komanduri S, Schechter S, Sleeper M (2014) Harder to ignore? revisiting pop-up fatigue and approaches to prevent it. In: 10th Symposium On Usable Privacy and Security (SOUPS 2014), pp. 105–111. USENIX Association, Menlo Park, CA
24. Raja F, Hawkey K, Hsu S, Wang KLC, Beznosov K (2011) A brick wall, a locked door, and a bandit: A physical security metaphor for firewall warnings. In: Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS '11, pp. 1:1–1:20
25. Gilfix M, Couch AL (2000) Peep (the network auralizer): Monitoring your network with sound. In: Proceedings of the 14th USENIX Conference on System Administration, LISA '00, pp. 109–118

26. Mark Ballora Nicklaus A. Giacobe DLH (2011) Songs of cyberspace: an update on sonifications of network traffic to support situational awareness
27. Axon L, Creese S, Goldsmith M, Nurse J (2016) Reflecting on the use of sonification for network monitoring. *ThinkMind*
28. Axon L, Nurse J, Goldsmith M, Creese S (2017) A formalised approach to designing sonification systems for network-security monitoring. *Int J Adv Secur* 10(1–2):26–47
29. Sonification of a network's self-organized criticality for real-time situational awareness. *Displays* **47**, 12 – 24 (2017). Sonification of Real-time Data
30. Debashi M, Vickers P (2018) Sonification of network traffic flow for monitoring and situational awareness. *PLoS ONE* 13(4):1–31
31. Hildebrandt T, Hermann T, Rinderle-Ma S (2016) Continuous sonification enhances adequacy of interactions in peripheral process monitoring. *Int J Hum Comput Stud* 95:54–65
32. Brown A, Martin M, Kapralos B, Green M, Garcia-Ruiz M (2009) Poster: Towards music-assisted intrusion detection. Oakland, USA
33. Qi L, Vargas Martin M, Kapralos B, Green M, García-Ruiz M (2007) Toward sound-assisted intrusion detection systems. In: Meersman R, Tari Z (eds) *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS*. Springer, Berlin Heidelberg, Berlin, Heidelberg, pp 1634–1645
34. Minakawa R, Takada T (2017) Exploring alternative security warning dialog for attracting user attention: Evaluation of “kawaii” effect and its additional stimulus combination. In: *Proceedings of the 19th International Conference on Information Integration and Web-based Applications & Services, iiWAS '17*, pp. 582–586
35. Terri L. Bonebright JHF (2011) Evaluation of auditory display. In: J.G.N. Thomas Hermann Andy Hunt (ed.) *The Sonification Handbook*, chap. 6. Iisd
36. Brewster S, Raty VP, Kortekangas A (1996) Earcons as a method of providing navigational cues in a menu hierarchy. In: Sasse MA, Cunningham RJ, Winder RL (eds) *People and Computers XI*. Springer, London, pp 169–183
37. Dingler T, Lindsay J, Walker BN, maximilians-universität München L (2008) Learnability of sound cues for environmental features: Auditory icons, earcons, spearcons, and speech. In: *Proceedings of the 14th International Conference on Auditory Display*. <http://sonify.psych.gatech.edu/publications/pdfs/2008ICAD-DinglerLindsayWalker.pdf>
38. Gaver WW (1986) Auditory icons: Using sound in computer interfaces. *Hum Comput Interact* 2(2):167–177
39. of Information Technology, D.: Benefits of assistive technology extend to everyone. Tech. rep., University of Wisconsin?Madison (2008). <https://it.wisc.edu/about/annual-reports/>
40. Fogg BJ, Soohoo C, Danielson DR, Marable L, Stanford J, Tauber ER (2003) How do users evaluate the credibility of web sites?: A study with over 2,500 participants. In: *Proceedings of the 2003 Conference on Designing for User Experiences, DUX '03*, pp. 1–15
41. Hostetler B (2016) Is your organization compromise ready? 2016 data security incident report. Tech. rep. <https://www.bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf>
42. Kelly R (2017) Almost 90% of Cyber Attacks are Caused by Human Error or Behavior. <https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/>
43. Sidler V (2017) Why phishing attacks are so effective. <https://businesstech.co.za/news/industry-news/206328/why-phishing-attacks-are-so-effective/>
44. CyberSponse: Phishing is Still Very Effective ? How Can That Be? (2015). <https://cybersponse.com/phishing-is-still-very-effective-how-can-that-be>
45. Hermann T, Hunt A, Neuhoﬀ JG (2011) *The sonification handbook*, pp. 105–106. Logos Verlag
46. Wickens CD, Lee J, Liu YD, Gordon-Becker S (2003) *Introduction to Human Factors Engineering*, 2nd edn. Prentice-Hall Inc, USA
47. visualping.io: Page monitor (2017). <https://chrome.google.com/webstore/detail/page-monitor/ogeebjpdeabhnjcjpfhgdbjajcjpeggg>
48. arlo.is: Gmail audio alerts (2018). <https://chrome.google.com/webstore/detail/gmail-audio-alerts/mneephebbcbchofepodkcknohneogkdc>
49. Wachete: Wachete - monitor website content changes (2017). <https://chrome.google.com/webstore/detail/wachete-monitor-website-c/oendfdlbglnmpmlpnokgopffmiphfgn>
50. freaktechnik: Notification sound (2018). <https://addons.mozilla.org/en-US/firefox/addon/notification-sound/?src=recommended>
51. bootleq: Noise - make sound response when event happen (2018). <https://addons.mozilla.org/en-US/firefox/addon/noise/>
52. Upson L (2010) Google Chrome Blog: An update on Chrome, the Web Store and Chrome OS. <https://chrome.googleblog.com/2010/12/update-on-chrome-web-store-and-chrome.html>
53. Saint N (2010) Google Launching “Chrome Web Store” (2010). <http://www.businessinsider.com/google-launching-chrome-web-store-2010-5>
54. Barth A, Felt AP, Saxena P, Boodman A (2010) Protecting Browsers from Extension Vulnerabilities. *Ndss* 147:1315–1329
55. Liu L, Zhang X, Inc V, Yan G, Chen S (2012) Chrome extensions: Threat analysis and countermeasures. In: *19th Network and Distributed System Security Symposium (NDSS '12)*
56. Google: What are extensions? - Google Chrome (2015). <https://developer.chrome.com/extensions>
57. Google Developer: Content Scripts (2015). https://developer.chrome.com/extensions/content_scripts
58. Google: JavaScript APIs - Google Chrome (2017). https://developer.chrome.com/extensions/api_index
59. Sunshine J, Egelman S, Almuhiemedi H, Atri N, Cranor LF (2009) Crying wolf: An empirical study of ssl warning effectiveness. In: *Proceedings of the 18th Conference on USENIX Security Symposium, SSYM'09*, pp. 399–416
60. Huang LS, Rice A, Ellingsen E, Jackson C (2014) Analyzing forged ssl certificates in the wild. In: *2014 IEEE Symposium on Security and Privacy*, pp. 83–97
61. Ahmed AA, Abdullah NA (2016) Real time detection of phishing websites. In: *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 1–6
62. Fang L, Bailing W, Junheng H, Yushan S, Yuliang W (2015) A proactive discovery and filtering solution on phishing websites. In: *2015 IEEE International Conference on Big Data (Big Data)*, pp. 2348–2355
63. Jo I, Jung E, Yeom HY (2010) You're not who you claim to be: Website identity check for phishing detection. In: *2010 Proceedings of 19th International Conference on Computer Communications and Networks*, pp. 1–6
64. Lee JI, Kim DH, Chang-Hoon L (2015) Heuristic-based Approach for Phishing Site Detection Using URL Features. *Adv Comput, Electron Electric Technol* pp. 131–135
65. Ludl C, Mcallister S, Kirda E, Kruegel C (2007) On the effectiveness of techniques to detect phishing sites. In: *Proceedings of the 4th International Conference on Detection of Intrusions*

- and Malware, and Vulnerability Assessment, DIMVA '07, pp. 20–39
66. Mohammad RM, Thabtah F, McCluskey L (2014) Intelligent rule-based phishing websites classification. *IET Inf Secur* 8(3):153–160
 67. Nguyen LAT, To BL, Nguyen HK, Nguyen MH (2014) A novel approach for phishing detection using url-based heuristic. In: 2014 International Conference on Computing, Management and Telecommunications (ComManTel), pp. 298–303
 68. V, PK, AK (2014) Performance study of classification techniques for phishing url detection. In: 2014 Sixth International Conference on Advanced Computing (ICoAC), pp. 135–139
 69. Jeeva SC, Rajsingh EB (2016) Intelligent phishing url detection using association rule mining. *Hum-centric Comput Inf Sci*. 6(1), 64:1–64:19
 70. Neuhoff J (2019) Is sonification doomed to fail? pp. 327–330
 71. Lutz OHM, Kröger JL, Schneiderbauer M, Kopankiewicz JM, Hauswirth M, Hermann T (2020) That password doesn't sound right: Interactive password strength sonification. In: Proceedings of the 15th International Conference on Audio Mostly, AM '20, p. 206–213. Association for Computing Machinery
 72. Axon LM, Alahmadi B, Nurse JR, Goldsmith M, Creese S (2018) Sonification in security operations centres: what do security practitioners think? arXiv preprint [arXiv:1807.06706](https://arxiv.org/abs/1807.06706)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.