Journal on Multimodal User Interfaces (2022) 16:399–412
https://doi.org/10.1007/s12193-022-00397-z

ORIGINAL PAPER


# Grouping and Determining Perceived Severity of Cyber-Attack Consequences: Gaining Information Needed to Sonify Cyber-Attacks

**Keith S. Jones[1] · Natalie R. Lodinger[1] · Benjamin P. Widlus[1] · Akbar Siami Namin[2] · Emily Maw[1] · Miriam Armstrong[1]**

Received: 3 May 2021 / Accepted: 28 September 2022 / Published online: 1 November 2022


**Abstract**
Cyber-attacks are a continuing problem. These attacks are problematic for users who are visually impaired and cannot rely on visual cues to indicate a potential cyber-attack. Sonification is an alternative way to help users who are visually impaired detect potential cyber-attacks. Sonification provides information to users using non-speech sounds. Sonification could provide users who are visually impaired with information on potential cyber-attack consequences that could stem from their actions. However, there are two challenges with sonifying cyber-attack consequences. First, there are many potential cyber-attack consequences to sonify, and humans have a limited ability to remember associations between sonifications and their meanings. Second, cyber-attack warning messages are better trusted when they align the severity of the consequences with the user's perceived severity. However, we do not know the perceived severity of individual consequences. Therefore, we need to reduce the number of consequences to sonify and to determine the perceived severity of these consequences. We had non-expert participants group cyber-attack consequences based on perceived similarity. Analyses revealed that participants' groupings formed seven clusters. We then had non-expert participants rate the perceived severity of each cyber-attack consequence. Those ratings were used to determine the perceived severity of each cluster. These efforts resulted in a set of cyber-attack consequence clusters that (a) is small enough that users should be able to remember associations between sonifications and their meanings, and (b) can be sonified in a way that reflects users' perceptions regarding the severity of the clustered cyber-attack consequences. As such, the results of these studies are critical steps towards creating effective sonifications that serve as cyber-security warning messages.

**Keywords** Warning message design · Cyber-attack consequences · Mental models · Cybersecurity

## 1 Introduction

Cyber-attacks are a consistent and costly threat. The United States Department of Homeland Security (2020) reports that ransomware attacks have increased since 2017 [1]. Recently, the COVID-19 pandemic led to an increase in spear-phishing attacks in which cyber-criminals pretended to be officials associated with the pandemic, such as the U.S. Centers for Disease Control and Prevention [1, 2]. Further, the reported losses from cybercrime attacks in 2018 was $2.7 billion, a sum that increased relative to losses in 2017 [1]. Therefore, cyber-attacks are numerous and costly.

### 1.1 The unique cyber-security challenges for users who are visually impaired

Users who are visually impaired could have difficulty detecting the potential for a cyber-attack because many existing cybersecurity indicators are visual and thus less usable for these users [3]. For example, websites contain several visual cues that speak to their legitimacy, such as the presence of a lock icon, the s in https, correctly spelled domain names, and a professional appearance [4]. Users who are visually impaired cannot easily use such visual cues to determine if a website is legitimate because they often rely on screen readers [5–8], which provide speech output of the text on a page and any text-descriptions of visual content, such as images, but cannot convey purely visual content [5, 7–10].

✉ Keith S. Jones
keith.s.jones@ttu.edu

[1] Department of Psychological Sciences, Texas Tech University, Lubbock, TX, USA

[2] Department of Computer Science, Texas Tech University, Lubbock, TX, USA

Additionally, when malicious webpages attempt to automatically install software on users' systems, users are provided a visual indicator that a download was initiated. Users who are visually impaired reported that the information they receive in such cases is insufficient to understand what is being downloaded or make an informed decision about whether to allow it to install [5]. Therefore, users who are visually impaired have unique challenges when navigating cybersecurity because they cannot rely on visual information about potential cyber-attacks.

### 1.2 A possible solution to the challenges experienced by users who are visually impaired

Sonification is the use of non-speech sounds to convey information to users about system behavior [8, 10–12]. Sonifications have been used to convey important messages or warnings in other contexts, including healthcare [13, 14], aircraft cockpits [13], weather forecasts [15], assistive technologies for users with language impairments [16, 17], monitoring machines in a factory [18], navigation [19–21], rehabilitation [22, 23] and athletic training [24–26]. Sonifications can be used in a purely auditory interface or in conjunction with interfaces that employ other modalities. See [27] for an example of using sonifications in conjunction with a haptic interface.

Sonifications can provide non-visual and non-speech information about potential cyber-attacks [28]. Because screen readers present written content as speech to users who are visually impaired, an advantage of providing warnings as sonifications rather than text-based messages is that warnings can be distinguished from content on the Internet [13]. Users who are visually impaired mainly hear speech from screen readers [5–8]. Therefore, providing warnings as text could overload users who are visually impaired with speech output. Using sonifications rather than text-based warnings can be advantageous for users who are visually impaired. As such, sonifications may help users who are visually impaired detect potential cyber-attacks and exhibit safe behaviors [3]. In addition, sonifications could benefit users who are not visually impaired but whose visual attention is already taxed.

### 1.3 The message to convey in sonifications

These sonifications should include certain characteristics to be effective warning messages. Three of these characteristics that will be addressed by the current paper are (1) they need to convey the consequences of the attack, (2) they need to convey the severity of the consequence, and (3) they need to convey the severity of the consequence in a way that aligns with the user's perceived severity of that consequence. The following paragraphs present the literature associated with each of these three aspects.

These sonifications should convey the consequences of a cyber-attack. Past studies found non-experts better understand and follow the advice of warning messages that explain the consequences of attacks rather than present attack descriptions [29, 30]. For instance, Kauer and colleagues found people were more likely to comply with a warning when they thought a personal risk was present [30]. The authors concluded that providing personal consequences rather than technical descriptions could lead people to better recognize and understand the personal risks [30]. Therefore, cyber-attack consequences should be sonified to allow users who are visually impaired to understand these sonified warnings.

However, even if the warning is understood, it may be ignored if the user perceived the consequences to not be severe. Therefore, information on the severity of the consequence should be included in the sonification. Dodel and Mesch found a positive relationship between perceived severity, which they defined as "the beliefs about the seriousness of the consequences of the condition [such] as the awareness of the cyber-threats' plausible consequences", and behaviors to avoid malware [31 p. 362]. This study's results suggest the more the user is aware of the consequences, the more likely they are to engage in behaviors that would prevent malicious attacks. Furthermore, Ng and colleagues found perceived severity affects the relationship of multiple variables and the likelihood of engaging in behaviors to prevent cyber-attacks [32]. Specifically, they found that users who think the consequence is severe are more likely to attempt a security practice and behavior to prevent the consequence (e.g., comply with a warning message) even if they doubt the effectiveness of that behavior [32]. Therefore, the perceived severity of cyber-attack consequences affects user's motivation to exhibit cybersecurity behaviors.

Lastly, the consequence and severity of that consequence need to align with the user's mental models of those aspects. Mental models in the current paper refers to participants' understanding and knowledge of the consequences and their perception of their severity (i.e., perceived severity). Bartsch and colleagues found one third of participants distrusted warnings they thought exaggerated the consequences or the potential of that attack [29]. This distrust may lead users to not feel a need to comply with the warning [29]. Additionally, they found participants thought certain consequences may be more pertinent to them than other consequences and different participants thought different consequences would be pertinent, suggesting users may not think all consequences are important enough to protect against [29]. Sonifications need to match the consequence and severity

of the consequence to users' mental models to avoid users distrusting the warning.

### 1.4 The current paper: A method to determine how to sonify cyber-attack consequences

Our long-term goal is to create sonifications that serve as cybersecurity warning messages. These sonifications will convey the consequences of the potential attack, the severity of those consequences, and do so in a way that aligns with users' mental models.

However, there are two main challenges that must be addressed to create these sonifications. These challenges and how we addressed them will be discussed in the following subsections.

#### 1.4.1 Challenge #1: Too many sonifications to remember

The first challenge is that there are so many potential consequences of cyber-attacks that people would find it difficult to remember the meaning of each sonification. Cyber-attacks can affect multiple aspects of a user's property and assets, such as their information (e.g., social security numbers), finances (e.g., monetary loss due to paying a ransom to recover lost assets), devices (e.g., loss of access to networks), or some combination thereof [33–35]. However, people can only remember the meaning of a limited number of sounds. For example, Brewster reported users could only remember the meaning of 8 to 9 of the sonifications tested immediately following and one week after training [16]. Additionally, he reported users could remember the meaning of about 11 compound sonifications, or multiple sounds combined using rules associated with their meaning [16]. Therefore, people would find it impossible to remember the meaning of sonifications if each cyber-attack consequence were to be sonified.

To address that challenge, we needed a way to reduce the number of consequences that would be sonified. One approach is to group similar consequences, and sonify each group. Toward that end, we had non-experts group cyber-attack consequences based on their perceived similarity. That effort is described in Sect. 2.

#### 1.4.2 Challenge #2: Lack of perceived severity information

The second challenge is that currently there is no information about how users perceive the severity of each cyber-attack consequence. For example, we do not know whether users perceive an attacker gaining the user's personal information as more or less severe than an attacker preventing the user from accessing their email. Without such information, we cannot construct effective sonifications so that the conveyed level of severity aligns with users' mental models.

To address that challenge, we had people rate the perceived severity of individual cyber-attack consequences. We then combined those individual ratings to determine perceived severity for each identified group of cyber-attack consequences. That effort is described in Sect. 3.

### 1.5 Outline

In the current paper, we take two important steps towards creating cybersecurity sonifications. In the first step, we identified groups of similar consequences that can be sonified. This step included creating cyber-attack consequences to be grouped and conducting a card sorting study to determine clusters of consequences that are perceived to be similar. In the second step, we conducted a study to determine the perceived severity of these clusters of consequences. This step included 33 participants rating the severity of the consequences written in Step 1. These ratings were used to determine the perceived severity of each cluster of consequences. The perceived severity can then be used to align the severity of the sonifications with the users' mental models.

## 2 Step 1: Grouping a list of consequences to sonify

### 2.1 Identifying consequences to be grouped

We identified 50 consequences that were framed in terms of consequences to the user from a list of cyber-attacks. We used the popular threat model created by Microsoft called STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) model to gain a list of potential attacks in each threat category. For example, the list of attacks for repudiation was digital signature forgery, email spoofing, man in the browser, logfile removal, log injection, collision attack, pre-image attack, and identity repudiation. We then created multiple descriptions of each attack. An example description of an email spoofing attack was "masquerading a trusted person through email". A human factors professor who is knowledgeable about human cognition and behavior used these attack descriptions to write consequences that aligned with recommendations from the risk communication literature. Therefore, the consequences were written so that non-expert users with no cybersecurity background could understand them. The consequences were framed in terms of consequences to the user and did not include technical terms as recommended by the risk communication literature [29, 30, 36]. As an example, the consequence for email spoofing was

**Table 1** The total number of attacks and consequences for each STRIDE category.

| STRIDE Category | Total Number of Attacks | Total Number of Consequences | Total Number of Unique Consequences |
|---|---|---|---|
| Spoofing | 12 | 9 | 7 |
| Tampering | 15 | 16 | 8 |
| Repudiation | 9 | 7 | 5 |
| Information Disclosure | 19 | 10 | 6 |
| Denial of Service | 25 | 14 | 11 |
| Elevation of Privilege | 22 | 11 | 2 |

"The cyber-attacker made you think that an email that you received from the attacker came from someone else." The full list of consequences can be found in Appendix A. We aimed to create an as inclusive as possible list of attacks, but we acknowledge that we may not have included every potential attack. The number of attacks and consequences we determined for each STRIDE category are presented in Table 1.

## 2.2 Using card sorting to group the consequences

### 2.2.1 Participants

Undergraduate students were recruited from a university participant pool. Thirty-three participants (11 male) participated and were compensated with partial course credit. The average age of these participants was 19.82 years ($SD = 6.24$) with their ages ranging from 18 to 54 years. Participants reported they were not experts in cybersecurity, meaning they had not held a job or taken a university course in the field. We did not anticipate differences between users who are sighted and those who are visually impaired in general perception of consequences. Therefore, we did not use individuals who are visually impaired as participants.

### 2.2.2 Materials

OptimalSort [37] was used for the card sorting task. Figure 1 presents the OptimalSort display. Each consequence was presented on a card on the left side of the screen. Participants formed groups in the white space on the right side of the screen. They started a new group by dragging a card from the left side into the white space. They could place cards into an existing group by moving it directly over a card on the right side. Participants could also name each group in the box that appeared above each group.

### 2.2.3 Procedure

Participants provided informed consent after arriving at the laboratory. The experimenter then explained the card sorting task. Participants were instructed to create groups of consequences they perceived to be similar. Each consequence could be used once. Participants were also told to avoid creating groups containing a single consequence.

Before sorting the consequences, the experimenter had the participant read all consequences out loud, which allowed participants to familiarize themselves with all consequences that needed to be sorted. Participants then began

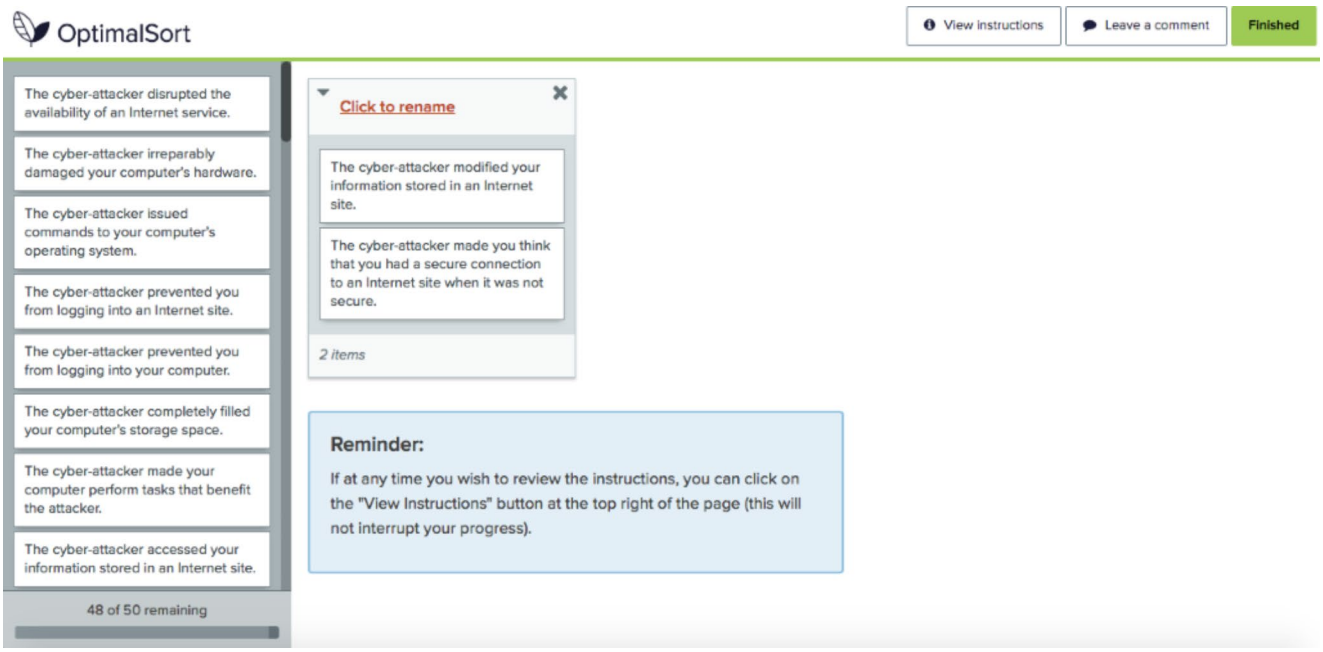


**Fig. 1** The OptimalSort Web application display with each consequence presented on a card (on the left) and space to create groups (on the right)

sorting the consequences. They were able to sort and resort consequences until they were content with their groups. Throughout the experiment, the instructions were available for participants to reference using the "View Instructions" button at the top of the page. Once participants were finished sorting the consequences, they gave each group a label, such as a word, phrase, or sentence, that represented the reason those consequences were grouped (i.e., the perceived similarity of the consequences). Some examples of labels are "Involves the attacker accessing and controlling computer programs and files", "potential damage for user", and "access".

After naming the groups of consequences, participants filled out a questionnaire about their age, gender, and experience in the cybersecurity field. Participants completed the experiment in less than one hour. The university Institutional Review Board approved the study.

#### 2.2.4 Results: Cluster Analysis

Across all participants, 226 groups of consequences were created. We first prepared the grouping data to be used in a cluster analysis. Using the participants' grouping data, we created binary variables in which a consequence received a one if it was present in the group and a zero if it was absent from that group. We used these variables to create a Jaccard similarity matrix to use in the clustering analysis. The Jaccard matrix was created by calculating the S-coefficient or the Jaccard coefficient of community using Eq. 1, in which a is the number of participants who placed two consequences in the same group, b is the number of participants who created a group with just the first consequence, and c is the number of participants who created a group with just the second consequence [38, 39]. Therefore, the Jaccard index represented how many groups the participants created with those two consequences out of the total number of groups created with those consequences. This index was also a measure of similarity between two consequences because the more times two consequences were placed in a group together, the larger the Jaccard index for those two consequences. We used this matrix of Jaccard indexes in the cluster analysis.

$$J = a/(a+b+c) \quad (1)$$

We used an unsupervised clustering algorithm, K-means, to cluster the consequences [40]. In K-means, the experimenter must select the number of clusters to create. The optimal number of clusters is the one where the items in each cluster are most similar to each other and most dissimilar to items in other clusters. In mathematical terms, the optimal number of clusters is the one that has the smallest total within cluster sums of squares. A small within cluster sum of squares indicates an optimal cluster structure.

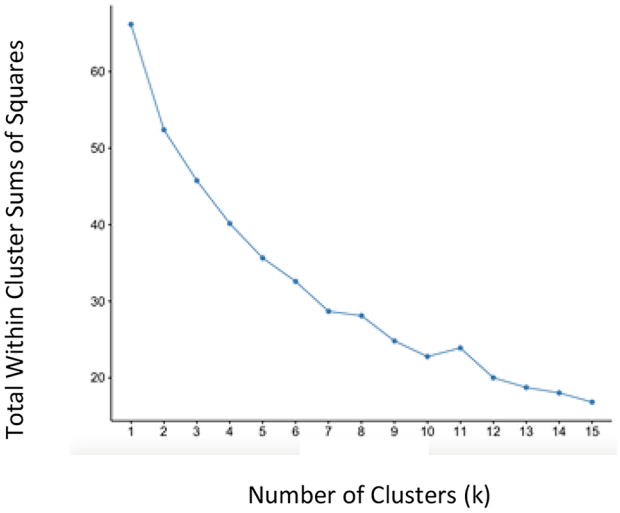


**Fig. 2** The plot used to determine seven clusters was the optimal solution using the elbow method.

We used the elbow method to determine the optimal number of clusters. In the elbow method, one examines a plot of the total within cluster sums of squares for different numbers of clusters for a bend (i.e., elbow) in the plot. One seeks to identify the number of clusters at which the curve becomes relatively flat compared to lesser numbers of clusters (i.e., the elbow). The elbow is the point at which adding another cluster does not substantially decrease the total within clusters sums of squares. In other words, adding another cluster does not lead to a better cluster solution than the prior number of clusters. The elbow plot used in the current study is presented in Fig. 2. We determined that a clustering solution with seven clusters was the optimal solution for our data because the steepest decline in total within clusters sums of squares occurs before the elbow at seven clusters. The decline in total within clusters sums of squares after seven clusters is more gradual than before seven.

We then clustered the consequences into these seven clusters using the K-means clustering algorithm. This cluster analysis allowed us to determine the consequences participants perceived to be similar because consequences are placed into clusters based on how similar they are to each other (i.e., how small the distance is between them). Therefore, consequences perceived by participants to be similar to one another were placed into the same cluster in the analysis. The datasets are available from the corresponding author on request.

#### 2.2.5 Results: Conceptually defining the clusters

The way the cards were sorted into these seven clusters appeared to be meaningful because we were able to conceptually define each cluster. These definitions encompassed as many of the consequences in each cluster as possible. These definitions became the labels for the clusters. The labels aligned with the recommendations of the risk communication literature (i.e., personal, concrete, and did not contain technical terms) [29, 30, 36]. Table 2 includes the consequences in each cluster and the label we created for each cluster.

To determine the meaning of these clusters, we identified the overarching consequence of the consequences in each cluster. We now describe that overarching consequence for each cluster.

Cluster One consists of consequences from emails the attacker sent. These consequences are from an early stage in the attack and do not consist of what the attacker would gain from the attack. This cluster represents attacks in which the attacker sends users emails that could lead to an attack if their request is granted.

Cluster Two focuses on consequences that deny the user access to a service. Users are either prevented from accessing the Internet or their computer, or, once they access this service, the service runs inefficiently. Cluster Two represents an attack in which the attacker disrupted users' access to their computer or the Internet.

Cluster Three consists of consequences of the attacker gaining information on the Internet and the user's computer. The consequences describe the specific information and access the attacker gained. They also suggest the attacker is in possession of the information, but do not describe what the attacker does with the information. Cluster Three represents an attack in which the attacker gained access to users' computers or one of their online accounts.

Cluster Four includes consequences mostly concerned with the attacker performing actions that benefit them and that occur without the user's awareness. The actions the attacker takes include modifying the user's equipment and files and preventing the user from using their computer. This cluster represents attacks in which the attacker alters users' computers or its contents to allow them to use it for their purposes without users knowing.

Clusters Five and Six represent attacks that occur through the Internet. Cluster Five includes consequences that focus on deception of the user via the Internet. Cluster Six includes consequences of the attacker using the Internet to modify or gain the user's information. The consequences describe how the attacker gains the information (e.g., interception) and the actions the attacker takes with the information (e.g., modifies, deletes). Cluster Five represents attacks in which the attacker manipulated users' use of or understanding about a website. Cluster Six represents an attack in which the attacker changed or intercepted information that users have on the Internet.

Cluster Seven includes consequences of an attack that affect the user's computer. Many consequences focus on affecting the computer's functioning, such as causing programs to crash or run slowly. This cluster represents attacks in which the attacker made users' computers operate inefficiently or not at all.

#### 2.2.6 Meaningful groupings of the consequences

Even though we perceived these clusters as meaningful, we needed to confirm that the seven-cluster solution was a valid cluster structure, meaning that the consequences were placed into meaningful and cohesive clusters. One method of doing so is using the silhouette method [41], which calculates the dissimilarity of a consequence within its cluster and all other consequences in the cluster structure (consequence silhouette width). Therefore, if the consequence is very similar to the consequences in its cluster and less similar to the consequences in other clusters, the consequence has been placed in the correct cluster. Silhouette widths can be calculated for each consequence, each cluster, and the entire cluster structure. For the cluster silhouette widths, an average of the silhouette widths for each consequence in the cluster is computed. For the overall cluster structure silhouette width, an average of the silhouette widths for all consequences in the cluster solution is computed. For the overall cluster structure silhouette width, researchers have created rules-of-thumb for determining the cluster structure strength. However, rules-of-thumb are subjective and usually only apply to the domain in which they were created.

A better method of determining the strength of the cluster structure is to conduct a Monte Carlo simulation of overall cluster structure silhouette widths based on the number of groups created in the current study. Rather than using a criterion that was subjectively derived from another domain, we based the strength of our cluster structure on the clustering that occurred in our study. We used a random sorting of the consequences into the number of groups formed in the study to determine a range of silhouette scores based on random groupings of these consequences. Therefore, the Monte Carlo simulation led to a method of evaluating cluster structure that was specific to our study and not a general rule-of-thumb.

We conducted a Monte Carlo simulation [42] to determine whether our clustering solution provided meaningful clusters. We created a simulation that would randomly organize the consequences into the same number of groups as arranged by our participants. For example, if a participant

**Table 2** The consequences in and the label created for each cluster.

| | |
|---|---|
| **Cluster 1 Label:** | **The attacker sent you emails that could lead to an attack if their request is granted** |
| Consequences: | The cyber-attacker made you think that an email that you received from the attacker came from someone else. |
| | The cyber-attacker sent you an email that asks you to click on a given Internet link. |
| | The cyber-attacker sent you an email that asks you to respond with certain personal information. |
| | The cyber-attacker floods your inbox with a very large number of emails. |
| **Cluster 2 Label:** | **The attacker disrupted your access to your computer or the Internet.** |
| Consequences: | The cyber-attacker disrupted the availability of an Internet service. |
| | The cyber-attacker prevented you from logging into an Internet site. |
| | The cyber-attacker shut down an Internet site that you were using. |
| | The cyber-attacker prevented you from accessing your home network. |
| | The cyber-attacker caused your Internet connection to run very slowly. |
| | The cyber-attacker prevented you from logging into your computer. |
| **Cluster 3 Label:** | **The attacker gained access to your computer or one of your online accounts.** |
| Consequences: | The cyber-attacker accessed your computer files. |
| | The cyber-attacker determined your password. |
| | The cyber-attacker gained information about the device that you use to create your home network. |
| | The cyber-attacker accessed your computer programs. |
| | The cyber-attacker took control over one of your financial accounts. |
| | The cyber-attacker gains your username and password for a given Internet site. |
| | The cyber-attacker saw what was presented on your computer screen. |
| | The cyber-attacker accessed your information stored in an Internet site. |
| **Cluster 4 Label:** | **The attacker altered your computer or its contents to allow them to use it for their purposes without you knowing.** |
| Consequences: | The cyber-attacker removed your computer files in order to hide their activities. |
| | The cyber-attacker modified your computer files in order to hide their activities. |
| | The cyber-attacker used your computer to store and distribute stolen software. |
| | The cyber-attacker made your computer perform tasks that benefit the attacker. |
| | The cyber-attacker changed a device's serial number. |
| | The cyber-attacker modified the content of a digital message without your awareness. |
| | The cyber-attacker made your computer think that your password was entered when it was not. |
| | The cyber-attacker prevented you from using your computer until you pay a ransom. |
| | The cyber-attacker completely filled your computer's storage space. |
| | The cyber-attacker forged a digital signature on an electronic document. |
| **Cluster 5 Label:** | **The attacker manipulated your use of or understanding about a website.** |
| Consequences: | The cyber-attacker made you think an Internet site that the attacker created was a legitimate Internet site. |
| | The cyber-attacker made you think that you had a secure connection to an Internet site when it was not secure. |
| | The cyber-attacker made you think that information sent to your Internet browser came from a trusted source. |
| | The cyber-attacker caused your request for a certain Internet page to actually take you to a different Internet page. |
| | The cyber-attacker changed the appearance of an Internet site. |
| | The cyber-attacker made an Internet page that you use act differently than intended. |
| | The cyber-attacker changed how an Internet service functions so as to benefit the attacker. |
| **Cluster 6 Label:** | **The attacker changed or intercepted information that you have on the Internet.** |
| Consequences: | The cyber-attacker modified your information within an Internet database. |
| | The cyber-attacker modified your information stored in an Internet site. |
| | The cyber-attacker deleted your information stored in an Internet site. |
| | The cyber-attacker opened new hidden pathways by which they can enter your system from the Internet. |
| | The cyber-attacker performed actions on an Internet site as if they were you. |
| | The cyber-attacker intercepted Internet traffic as it passes between your computer and the Internet. |
| | The cyber-attacker gained information about existing hidden pathways by which they can enter your system from the Internet. |
| | The cyber-attacker rerouted your Internet requests to a device that they control. |
| **Cluster 7 Label:** | **The attacker made your computer operate inefficiently or not at all.** |
| Consequences: | The cyber-attacker caused your computer to run very slowly. |
| | The cyber-attacker caused your computer program to run very slowly. |
| | The cyber-attacker caused your computer to crash. |
| | The cyber-attacker caused a program on your computer to crash. |
| | The cyber-attacker irreparably damaged your computer's hardware. |
| | The cyber-attacker made your computer run software that your computer did not intend to run. |
| | The cyber-attacker issued commands to your computer's operating system. |

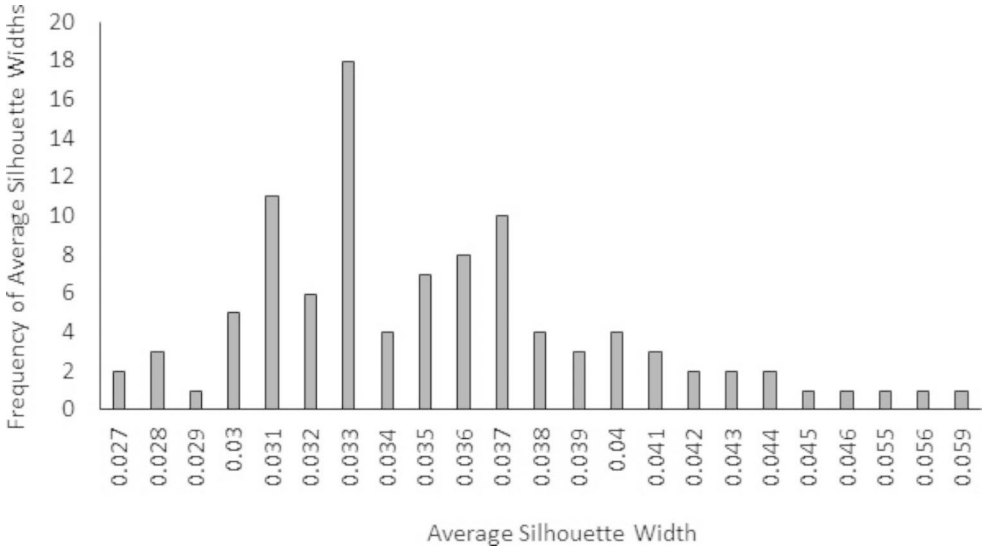


**Fig. 3** The frequency of each average silhouette width from the Monte Carlo simulation.

created four groups of consequences, the simulation would place the consequences into four groups. For each simulated participant, the consequences were organized into groups without replacement, meaning once a consequence was placed into a group, it could not be used again. Once the consequences were randomly placed into groups, the simulation created a Jaccard matrix from these random groupings of the consequences. The Jaccard matrix is a measure of the similarity between two consequences for that dataset and is calculated by dividing the number of times two consequences were grouped together by the total number of times each consequence was grouped. This Jaccard matrix was then used in K-means clustering. We specified that seven clusters should be created with the K-means method to match the seven-cluster solution from the previous analysis (i.e., the cluster analysis with actual participant data). After creating the seven-cluster solution, the simulation calculated the average silhouette width of this cluster solution. The simulation was run 100 times. The end product was a distribution of the average silhouette widths from the random organization of the consequences. The frequency of the average silhouette widths from the simulation can be seen in Fig. 3. The range of the average silhouette widths from the random groupings (silhouette width range from random groupings = 0.027–0.059) were much lower than the average silhouette width from the participants' data (silhouette width from participant data = 0.21). Therefore, the silhouette width of the cluster structure using participants' groupings is larger than a silhouette width from random groupings of the consequences, indicating that there is a clustering structure and that this structure is meaningful.

### 2.3 A Summary of Step 1

In Step 1, our goal was to reduce the number of cyber-attack consequences to a number that could be memorable as sonifications. We did so by having non-expert users group 50 consequences that covered the STRIDE model of cyber-attacks. This resulted in seven clusters of cyber-attack consequences that non-expert users perceive to be similar. Due to confirmatory analyses we conducted, we are confident in the validity of these seven clusters.

## 3 Step 2: Gaining information about consequence severity

In Step 1, the consequences of cyber-attacks were clustered to reduce the number of sonifications to a memorable amount. However, we also need to include the perceived severity of these consequences in the sonification. In Step 2, we determined the perceived severity of these clusters of consequences. The perceived severity would allow us to align the severity conveyed in the sonification to users' mental models of their severity.

### 3.1 Participants

Two hundred and one undergraduate students were recruited through introductory psychology courses. These participants had not participated in Step 1. They received partial course credit for participating in the study. Thirty-four participants had missing data or responded carelessly. Therefore, 167 participants' data (99 females, 1 gender unknown) were used in the analyses. The average age of these participants was 20.77 years (SD = 3.33) with their ages ranging from 17 to 41 years. Participants reported they were not

**Table 3** The number of consequences in each cluster of the 7-cluster structure.

| Cluster | Total Number of Consequences |
|---|---|
| 1 | 4 |
| 2 | 6 |
| 3 | 8 |
| 4 | 10 |
| 5 | 7 |
| 6 | 8 |
| 7 | 7 |

**Table 4** The mean, standard deviation, and results of the Tukey test for the perceived severity ratings.

| Cluster | Mean Severity Rating (SD) |
|---|---|
| 3 | 5.73(1.19)[a] |
| 4 | 5.63(1.25)[ab] |
| 6 | 5.51(1.30)[b] |
| 7 | 5.29(1.25)[c] |
| 5 | 4.99(1.39)[d] |
| 2 | 4.91(1.40)[d] |
| 1 | 4.78(1.63)[d] |

[abcd] These letters represent the results of the Tukey HSD test. Means with different letters were significantly different from one another

experts in cybersecurity, meaning they had not held a job or taken a university course in the field.

### 3.2 Procedure

Participants completed the study online on Qualtrics. Participants completed informed consent on the site. They then rated the 50 consequences for perceived severity. When rating these consequences, they considered the worst possible outcome of the consequence. For rating perceived severity, participants used a 7-point Likert scale that ranged from 1 "not severe" to 7 "severe" [43]. After providing all ratings, participants completed a demographics survey that included questions about their gender, age, and whether they had taken a college level cybersecurity course or worked in this field. This study was approved by the university Institutional Review Board.

### 3.3 Results and discussion

We removed participants who did not complete the entire study (32 participants) or responded with the same answer choice to all questions (i.e., careless responders; two participants) [44]. Therefore, 167 participants were included in the analyses. In this section, we describe analyses based on the seven clusters. However, the means and standard deviations of the perceived severity ratings for the individual consequences can be found in Appendix A.

#### 3.3.1 Perceived severity of the 7 clusters

We wanted to determine the perceived severity for each cluster. To do so, we placed each consequence into the cluster to which it belonged based on the cluster structure from Step 1. Each consequence was only placed into one cluster. As seen in Table 3, the number of consequences in each cluster was unequal.

Once the consequences were divided into their respective clusters, we needed to calculate the perceived severity for these clusters. First, we determined each participant's perceived severity rating for each cluster. We did so by averaging each participant's severity ratings for the consequences in each cluster. For example, for each participant, we averaged the severity ratings for the four consequences in Cluster 1. This gave us each participant's perceived severity rating for each cluster. We then used the perceived severity ratings for each participant to determine the overall perceived severity for each cluster. The perceived severity ratings for each participant were averaged to provide an overall perceived severity rating for each cluster. These mean perceived severity ratings are presented in Table 4.

We determined how the ratings of perceived severity differed between the seven clusters. This analysis would allow us to know which sonifications need to convey greater severity than the sonifications of other clusters. We conducted a one-way analysis of variance (ANOVA) with cluster as the independent variable and mean severity rating as the dependent variable. The seven clusters differed in perceived severity, $F(6, 966) = 54.49$, $p < .001$, $\eta_p^2 = 0.25$. We then conducted a Tukey HSD test to determine which clusters differed in perceived severity. As represented in Table 4, participants perceived the consequences in Clusters 1, 2, and 5 as less severe than the consequences in the other clusters. The consequences of Clusters 3 and 4 were perceived to be the most severe. These results can be used to match the perceived severity to the severity presented in the warning message. For example, the sonifications for Clusters 3 and 4 should convey great severity whereas the sonifications for Clusters 1, 2, and 5 should convey less severity.

## 4 Summary

The goal of these studies was to address two challenges in creating sonifications as cyber-security warning messages. The first challenge was reducing the number of cyber-attack consequences to sonify. The second challenge was determining the perceived severity for these consequences. We

addressed these challenges in two steps. In the first step, we had participants group cyber-attack consequences by perceived similarity to reduce the number of items to sonify. In the second step, we had participants rate the perceived severity of each consequence to determine the perceived severity of these groups of consequences.

In Step 1, we found 7 clusters of cyber-attack consequences. We also determined the main characteristics of the attacks in each cluster and created a label to reflect those characteristics. We can then create a sonification for the main characteristics of each cluster to be used as warning messages for users who are visually impaired. For example, for Cluster 2, for which the overarching consequence is "The attacker disrupted your access to your computer or the Internet.", we can find sounds that would be associated with blocking access to indicate that the user's current behavior could lead to an attack that would prevent them from accessing their computer or Internet. These clusters allow us to make a small number of auditory warning messages that can be distinguished and alert people to many cyber-attack consequences. The warning messages will also be understood by users because they will be sonifications of personal consequences rather than technical descriptions of attacks. These clusters should allow us to create auditory warning messages.

In Step 2, we determined the perceived severity of each cluster. Clusters 3, 4, 6, and 7 were perceived as more severe than Clusters 1, 2, and 5. This result suggests users do not perceive all consequences of cyber-attacks to be equal in severity. Bartsch and colleagues found non-experts thought financial losses were more important than other consequences [29]. However, the current study expands on this literature and demonstrates people view access or alterations to their device and information (Clusters 3, 4, 6, and 7) as more severe than malicious emails, disrupted access to websites, or manipulated websites (Clusters 1, 2, 5). The current study also provides severity ratings for many consequences. With these perceived severity ratings, we can convey the appropriate amount of severity in these sonifications.

These ratings can be used to match the perceived severity of the consequences in the cluster to the perceived severity of the sonifications in the warning messages. For example, increasing the frequency of the sound throughout the time it is played leads people in multiple countries to perceive the sound as indicating danger [45]. Therefore, a sonification that increases in frequency could be used to indicate the cluster with consequences perceived to be more dangerous or severe, such as Cluster 3. Bartsch and colleagues found people reported distrusting warning messages when they perceived the consequences described in the message to be exaggerated or questionable [18]. Therefore, aligning the severity conveyed in the warning message to the user's mental model should encourage users to trust and comply with the warning message.

In addition to the aforementioned contributions, the present paper also provides information about the perceived severity of individual cyber-attack consequences (Appendix A). This information is useful to practitioners creating text-based warning messages. The warning message literature recommends providing the severity of the consequences and matching that severity to people's perceived severity of that consequence [29, 31]. However, prior to this paper, information about the perceived severity of individual cyber-attack consequences was not known. Practitioners can use the perceived severity ratings to align the description of attack severity in the warning message with people's mental models of severity of that consequence. For example, a warning message about an attacker gaining the user's information from a website should present the consequence as severe to align with user's mental models. However, a warning message about an attacker changing the appearance of a website should be presented as less severe to align with users' mental models. The current study provides the information needed to create warning messages that align with user's mental models of cyber-attack consequence severity.

## 5 Limitations

One limitation of the perceived severity ratings is that we did not observe the behaviors of participants in response to these attacks. Although participants' self-report responses to these clusters suggest they perceive these groups of consequences differently, these data do not show their behavior would differ when confronted with consequences from different clusters. Future research should examine whether user behavior changes when cyber-attack consequences differ in perceived severity.

Furthermore, we gathered data from a homogenous population. All participants were college students and a majority were in their late teens or early twenties. Previous research found people held different mental models and exhibited different cybersecurity behaviors based on age and education level [31, 46]. Therefore, future research should investigate differences in perceived severity between the seven clusters of consequences with a population more varied in age and education.

## 6 Conclusion and future directions

The current paper takes two important steps towards sonifying cyber-security warning messages. In Step 1, clusters of similar cyber-attack consequences were determined. These

clusters can be used to create sonified warning messages about these consequences. In Step 2, the perceived severity rating of these clusters was determined. These severity ratings will allow us to align the perceived severity of the clusters of consequences with the severity indicated by the sonification. The results of these studies are critical steps towards creating sonifications that serve as cyber-security warning messages.

The next steps in this project are three-fold. First, we must validate the results of Step 1 and Step 2 with users who are visually impaired. The present methods and results provide a good starting point for such validation studies. Second, we must create and test sonifications that represent the consequences in each of the 7 clusters. To do so, we will identify sets of sounds that represent each cluster of cyber-attack consequences. For example, Cluster 2 includes consequences concerning disrupting access to the Internet or computer. To sonify this cluster, we will identify various sounds that convey a lack of access, such as the sound of a slamming door. Identifying such sounds will be non-trivial due to the difficulty of mapping meanings to sounds (see [47] for a review). We will employ multiple sonification mapping techniques to increase the likelihood that we will identify useful meaning-to-sound mappings. We will then conduct tests to identify which of those sounds most clearly represents Cluster 2. Third, we must create and test various ways to modify those sounds to convey perceived consequence severity. One possibility is to alter the frequency of those sounds to convey more or less severity. For example, Clusters 3, 4, 6, and 7 can have increasing frequencies. The frequency of the sound for Cluster 3 could also increase at a faster rate than the other three clusters to indicate it is more severe than the other three clusters. Clusters 1, 2, and 5 can have frequencies that are constant to convey these are not as severe. Alternatively, one could manipulate the salience of sonifications [48], positioning sonifications of clusters that were perceived as more severe in the foreground and those perceived as less severe in the background. Using such techniques, the sonifications would convey consequence severity in a way that aligns with users' mental models of consequence severity. Once various ways to modify the sounds are identified, we will then conduct tests to determine which sonification approach most clearly conveyed perceived severity.

## 7 Appendix A

| Consequence | Mean(SD) | 95% Lower CL | 95% Upper CL |
|---|---|---|---|
| The cyber-attacker accessed your computer files. | 5.77(1.46) | 5.55 | 6.00 |
| The cyber-attacker accessed your computer programs. | 5.50(1.50) | 5.27 | 5.73 |
| The cyber-attacker accessed your information stored in an Internet site. | 5.64(1.54) | 5.40 | 5.88 |
| The cyber-attacker caused a program on your computer to crash. | 5.17(1.67) | 4.91 | 5.42 |
| The cyber-attacker caused your computer program to run very slowly. | 4.55(1.85) | 4.27 | 4.83 |
| The cyber-attacker caused your computer to crash. | 5.66(1.51) | 5.43 | 5.89 |
| The cyber-attacker caused your computer to run very slowly. | 4.51(1.76) | 4.24 | 4.78 |
| The cyber-attacker caused your Internet connection to run very slowly. | 4.47(1.79) | 4.21 | 4.75 |
| The cyber-attacker caused your request for a certain Internet page to actually take you to a different Internet page. | 4.62(1.69) | 4.36 | 4.87 |
| The cyber-attacker changed a device's serial number. | 5.13(1.78) | 4.85 | 5.40 |
| The cyber-attacker changed how an Internet service functions so as to benefit the attacker. | 5.31(1.58) | 5.07 | 5.55 |
| The cyber-attacker changed the appearance of an Internet site. | 4.27(1.83) | 3.99 | 4.55 |
| The cyber-attacker completely filled your computer's storage space. | 5.32(1.63) | 5.07 | 5.57 |
| The cyber-attacker deleted your information stored in an Internet site. | 4.90(1.81) | 4.63 | 5.18 |
| The cyber-attacker determined your password. | 5.95(1.35) | 5.74 | 6.15 |
| The cyber-attacker disrupted the availability of an Internet service. | 4.72(1.71) | 4.46 | 4.98 |
| The cyber-attacker floods your inbox with a very large number of emails. | 4.49(1.85) | 4.20 | 4.77 |
| The cyber-attacker forged a digital signature on an electronic document. | 6.04(1.51) | 5.80 | 6.27 |
| The cyber-attacker gained information about existing hidden pathways by which they can enter your system from the Internet. | 5.73(1.51) | 5.50 | 5.96 |
| The cyber-attacker gained information about the device that you use to create your home network. | 5.50(1.56) | 5.26 | 5.74 |
| The cyber-attacker gains your username and password for a given Internet site. | 5.86(1.47) | 5.64 | 6.09 |
| The cyber-attacker intercepted Internet traffic as it passes between your computer and the Internet. | 5.26(1.53) | 5.02 | 5.49 |
| The cyber-attacker irreparably damaged your computer's hardware. | 6.13(1.51) | 5.90 | 6.36 |

| Consequence | Mean(SD) | 95% Lower CL | 95% Upper CL |
|---|---|---|---|
| The cyber-attacker issued commands to your computer's operating system. | 5.70(1.42) | 5.48 | 5.92 |
| The cyber-attacker made an Internet page that you use act differently than intended. | 4.77(1.74) | 4.51 | 5.04 |
| The cyber-attacker made you think an Internet site that the attacker created was a legitimate Internet site. | 5.28(1.57) | 5.04 | 5.52 |
| The cyber-attacker made you think that an email that you received from the attacker came from someone else. | 5.28(1.66) | 5.02 | 5.53 |
| The cyber-attacker made you think that information sent to your Internet browser came from a trusted source. | 5.40(1.52) | 5.17 | 5.63 |
| The cyber-attacker made you think that you had a secure connection to an Internet site when it was not secure. | 5.28(1.64) | 5.03 | 5.53 |
| The cyber-attacker made your computer perform tasks that benefit the attacker. | 5.63(1.49) | 5.40 | 5.86 |
| The cyber-attacker made your computer run software that your computer did not intend to run. | 5.30(1.53) | 5.06 | 5.53 |
| The cyber-attacker made your computer think that your password was entered when it was not. | 5.26(1.66) | 5.00 | 5.51 |
| The cyber-attacker modified the content of a digital message without your awareness. | 5.42(1.60) | 5.17 | 5.66 |
| The cyber-attacker modified your computer files in order to hide their activities. | 5.57(1.50) | 5.34 | 5.80 |
| The cyber-attacker modified your information stored in an Internet site. | 5.36(1.59) | 5.12 | 5.60 |
| The cyber-attacker modified your information within an Internet database. | 5.40(1.60) | 5.16 | 5.65 |
| The cyber-attacker opened new hidden pathways by which they can enter your system from the Internet. | 5.78(1.45) | 5.56 | 6.00 |
| The cyber-attacker performed actions on an Internet site as if they were you. | 5.82(1.57) | 5.58 | 6.06 |
| The cyber-attacker prevented you from accessing your home network. | 5.36(1.62) | 5.11 | 5.61 |
| The cyber-attacker prevented you from logging into an Internet site. | 4.88(1.71) | 4.62 | 5.14 |
| The cyber-attacker prevented you from logging into your computer. | 5.49(1.61) | 5.24 | 5.73 |
| The cyber-attacker prevented you from using your computer until you pay a ransom. | 6.20(1.55) | 5.96 | 6.43 |
| The cyber-attacker removed your computer files in order to hide their activities. | 5.65(1.55) | 5.42 | 5.89 |
| The cyber-attacker rerouted your Internet requests to a device that they control. | 5.84(1.44) | 5.62 | 6.06 |
| The cyber-attacker saw what was presented on your computer screen. | 5.17(1.84) | 4.89 | 5.45 |
| The cyber-attacker sent you an email that asks you to click on a given Internet link. | 4.32(2.03) | 4.01 | 4.63 |
| The cyber-attacker sent you an email that asks you to respond with certain personal information. | 5.02(1.97) | 4.72 | 5.33 |
| The cyber-attacker shut down an Internet site that you were using. | 4.51(1.78) | 4.24 | 4.79 |
| The cyber-attacker took control over one of your financial accounts. | 6.47(1.37) | 6.26 | 6.68 |
| The cyber-attacker used your computer to store and distribute stolen software. | 6.13(1.47) | 5.91 | 6.36 |

**Funding** This research was funded by the National Science Foundation [grant number 1564293].

**Data Availability** The corresponding author will have the data. All data support our published claims and comply with field standards.

**Code Availability** Not applicable.

## Declarations

**Conflicts of interest/Competing interests** None.

**Ethics approval** The university Institutional Review Board approved this study.

**Consent to participate** All participants provided informed consent to participate.

**Consent for publication** All authors agree to the publication of this paper.

## References

1. United States Department of Homeland Security (2020) Homeland Threat Assessment. https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf. Accessed 3 March 2021
2. Centers for Disease Control and Prevention (2021) COVID-19 Related Phone Scams and Phishing Attacks. https://www.cdc.gov/media/phishing.html. Accessed 3 March 2021
3. 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, pp. 2306–2313. https://doi.org/10.1145/2851581.2892363
4. Alsharnouby M, Alaca F, Chiasson S (2015) Why phishing still works: User strategies for combating phishing attacks. Int J Hum Comput Stud 82:69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005
5. Holman J, Lazar J, Feng J (2008) Investigating the security-related challenges of blind users on the Web. In: Langdon P, Clarkson J, Robinson P (eds) Designing inclusive futures. Springer, London, pp 129–138

6. Inan FA, Namin AS, Pogrund RL, Jones KS (2016) Internet use and cybersecurity concerns of individuals with visual impairments. J Educational Technol Soc 19:28–40
7. Lazar J, Allen A, Kleinman J, Malarkey C (2007) What frustrates screen reader users on the Web: A study of 100 blind users. Int J Hum Comput Interact 22:247–269. https://doi.org/10.1080/10447310709336964
8. Csapó Á, Wersényi G, Nagy H, Stockman T (2015) A survey of assistive technologies and applications for blind users on mobile platforms: a review and foundation for research. J Multimodal User Interfaces 9(4):275–286
9. Murphy E, Kuber R, McAllister G, Strain P, Yu W (2008) An empirical investigation into the difficulties experienced by visually impaired Internet users. Univ Access Inf Soc 7:79–91. https://doi.org/10.1007/s10209-007-0098-4
10. Zhao H, Plaisant C, Shneiderman B, Lazar J (2006) A framework for auditory data exploration and evaluation with geo-referenced data sonification. Manuscript under review
11. Walker BN, Nees MA (2011) Theory of Sonification. In: Hermann T, Hunt A, Neuhoff JG (eds) The Sonification Handbook. Logos Verlag, Berlin, Germany, pp 9–39
12. Vickers P (2016) Sonification and music, music and sonification. The Routledge Companion to Sounding Art. Routledge, London, pp 135–144
13. Guillaume A (2011) Intelligent auditory alarms. In: Hermann T, Hunt A, Neuhoff JG (eds) The Sonification Handbook. Logos Verlag, Berlin, Germany, pp 493–508
14. Aldana Blanco AL, Grautoff S, Hermann T (2020) ECG sonification to support the diagnosis and monitoring of myocardial infarction. J Multimodal User Interfaces 14(2):207–218
15. Hermann T, Drees JM, Ritter H(2003) Broadcasting auditory weather reports – a pilot project. In Brazil E, Shinn- Cunningham B (eds) Proceedings of the 2003 International Conference on Auditory Display. Boston University Publications Production Department, Boston, pp. 208–211
16. Brewster SA (1998) Using non-speech sounds to provide navigation cues. ACM Trans Computer-Human Interact 5:224–259. https://doi.org/10.1145/292834.292839
17. Ma X, Fellbaum C, Cook PR(2010) SoundNet: Investigating a language composed of environmental sounds. In: CHI 2010: Proceedings of the SIGCHI Conference on Huma Factors in Computing Systems. ACM, pp. 1945–1954. https://doi.org/10.1145/1753326.1753620
18. Gaver WW, Smith RB, O'Shea T(1991) Effective sounds in complex systems: The arkola simulation. In: Proceedings of CHI. ACM, New York, pp. 85–90
19. Ziemer T, Schultheis H (2019) Psychoacoustic auditory display for navigation: an auditory assistance system for spatial orientation tasks. J Multimodal User Interfaces 13(3):205–218
20. Skulimowski P, Owczarek M, Radecki A, Bujacz M, Rzeszotarski D, Strumillo P (2019) Interactive sonification of U-depth images in a navigation aid for the visually impaired. J Multimodal User Interfaces 13(3):219–230
21. El-Shimy D, Grond F, Olmos A, Cooperstock JR (2012) Eyes-free environmental awareness for navigation. J Multimodal User Interfaces 5(3):131–141
22. Newbold J, Gold NE, Bianchi-Berthouze N (2020) Movement sonification expectancy model: leveraging musical expectancy theory to create movement-altering sonifications. J Multimodal User Interfaces 14(2):153–166
23. Horsak, B., Dlapka, R., Iber, M., Gorgas, A. M., Kiselka, A., Gradl, C., … Doppler,J. (2016). SONIGait: a wireless instrumented insole device for real-time sonification of gait. *Journal on Multimodal User Interfaces*, *10*(3), 195–206
24. Stahl B, Thoshkahna B (2016) Design and evaluation of the effectiveness of a sonification technique for real time heart-rate data. J Multimodal User Interfaces 10(3):207–219
25. Dubus G (2012) Evaluation of four models for the sonification of elite rowing. J Multimodal User Interfaces 5(3):143–156
26. Lorenzoni V, Van den Berghe P, Maes PJ, De Bie T, De Clercq D, Leman M (2019) Design and validation of an auditory biofeedback system for modification of running parameters. J Multimodal User Interfaces 13(3):167–180
27. Frid E, Moll J, Bresin R, Sallnäs Pysander EL (2019) Haptic feedback combined with movement sonification using a friction sound improves task performance in a virtual throwing task. J Multimodal User Interfaces 13(4):279–290
28. Datta P, Namin AS, Jones KS, Hewett R (2021) Warning users about cyber threats through sounds. SN Appl Sci 3(7):1–21
29. Bartsch S, Volkamer M, Theuerling H, Karayumak F(2013) Contextualized web warnings and how they cause distrust. In: Huth M, Asokan N, Capkun S, Flechais I, Coles-Kemp L (eds) International Conference on Trust and Trustworthy Computing, Springer, Berlin, Heidelberg, pp. 205–222. https://doi.org/10.1007/978-3-642-38908-5_16
30. Kauer M, Pfeiffer T, Volkamer M, Theuerling H, Bruder R (2012) It is not about the design – it is about the content! Making warnings more efficient by communicating risks appropriately. GI-Edition – Lecture Notes in Informatics
31. Dodel M, Mesch G (2017) Cyber-victimization preventive behavior: a health belief model approach. Comput Hum Behav 68:359–367. https://doi.org/10.1016/j.chb.2016.11.044
32. Ng B, Kankanhalli A, Xu Y (2009) Studying users' computer security behavior: a health belief perspective. Decis Support Syst 46:815–825. https://doi.org/10.1016/j.dss.2008.11.010
33. Narwal B, Mohapatra AK, Usmani KA (2019) Towards a taxonomy of cyber threats against target applications. J Stat Manage Syst 22:301–325. https://doi.org/10.1080/09720510.2019.1580907
34. Federal Bureau of Investigation (2021) The Cyber Threat. https://www.fbi.gov/investigate/cyber. Accessed 3 March 2021
35. Federal Bureau of Investigation (2021) Ransomware. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware. Accessed 3 March 2021
36. Bartsch S, Volkamer M (2013) Effectively communicate risks for diverse users: A mental-models approach for individualized security interventions. Informatik 2013 – informatic angepasst an Mensch, Organisation und Umwelt. Boon, Gesellschaft Fur Informatik e.V., pp 1971–1984
37. Optimal Workshop Ltd (2021) https://www.optimalworkshop.com
38. Jaccard P (1912) The distribution of the flora in the alpine zone. New Phytol 11:37–50. https://doi.org/10.1111/j.1469-8137.1912.tb05611.x
39. Kaufman L, Rousseeuw PJ (2009) Finding groups in data: An introduction to cluster analysis. John Wiley & Sons, Hoboken
40. MacQueen J(1967) Some methods for classification and analysis of multivariate observations. In: Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability, pp. 281–297
41. Rousseeuw PJ (1987) Silhouettes: a graphical aid to the interpretation and validation of cluster analysis. J Comput Appl Math 20:53–65. https://doi.org/10.1016/0377-0427(87)90125-7
42. Sawilowsky SS (2003) You think you've got trivials? J Mod Appl Stat Methods 2:218–225. https://doi.org/10.22237/jmasm/1051748460
43. Likert R (1932) A technique for the measurement of attitudes. Archives of Psychology 140:1–55

44. Johnson JA (2005) Ascertaining the validity of individual protocols from web-based personality inventories. J Res Personality 39:103–129. https://doi.org/10.1016/j.jrp.2004.09.009
45. Kuwano S, Namba S, Schick A et al (2007) Subjective impression of auditory danger signals in different countries. Acoust Sci & Tech 28:360–362. https://doi.org/10.1250/ast.28.360
46. Wash R, Rader E(2015) Too much knowledge? Security beliefs and protective behaviors among United States Internet Users. In: SOUPS. The USENIX Association, pp. 309–325
47. Roddy S, Bridges B (2020) Mapping for meaning: the embodied sonification listening model and its implications for the mapping problem in sonic information design. J Multimodal User Interfaces 14(2):143–151
48. Tordini F, Bregman AS, Cooperstock JR (2016) Prioritizing foreground selection of natural chirp sounds by tempo and spectral centroid. J Multimodal User Interfaces 10(3):221–234