Analysis of Human-Computer Interaction Implication in Cyber Security

Jeffrey Grant
Department of Computer Science
Hampton University
jchasegrant@gmail.com

Chutima Boonthum-Denecke
Department of Computer Science
Hampton University
chutima.boonthum@hamptonu.edu

ABSTRACT

This report was made to develop a deeper understanding of what could be done to help better protect computer systems through ways other than simply creating programs. Human error, negligence, and apathy are also problems when it comes to preventing issues with safely browsing the internet or preventing cyber-attacks. Warnings can become too wordy, not be concise enough, not be present enough to notice, and these basic issues can cause even bigger problems.

When the layout and functions of a website or an operating system become unclear, there's an entire branch of computer science principles that can be utilized to make it manageable for people to use, and that is where Human-Computer Interaction (HCI) comes in. By analyzing what makes specific HCI principles effective, the potential to reduce, or possibly eliminate, flaws within cyber security caused by users or perpetuated by poor design choices by the creator.

CCS CONCEPTS

• **Systems Analysis ➜ Human–Computer Interaction** ➜ Understanding Human-Computer Interaction (HCI) • **Security and Privacy → Computer System Security** → Personal Security

KEYWORDS

Human-Computer Interaction (HCI), design, website, software, security

ACM Reference format:
J. Grant, C. Boonthum. 2021. SIG Proceedings Paper in word Format. In *Proceedings of 2021 ADMI Symposium, .*

1. INTRODUCTION

Throughout the internet's existence as a public platform where people could advertise products, and sometimes even themselves, and create domains that were visible to the world, there has been the concept of designing them in a way that would make it accessible for all those who came across it to achieve its goal efficiently. Even before the internet and operating systems was navigated primarily visually and through GUI, HCI was around in the late 70s as readable lines of text that helped guide the user through the experience of using the machine to accomplish their goals. Even before computers were able to be used by people other than developers and committed hobbyists, it existed as a means of improving piloting and mechanical operation. HCI was, and still is, fundamental to creating an environment in which anyone can make use of a computer system or web service, and based on the times of the information age, it's a must for just about everyone.

HCI, or more specifically effective HCI, can be identified through a set of implementation methods and principles. The implementation methods are universal, and range from Graphical User Interfaces, or GUIs, which can be extended into the idea of interfaces for touch screen enabled devices or devices that communicate between the user and the machine through voice. HCI not only determines if the layout and navigation methods for these websites and software, but also how it should respond to the user's input and where it should place those responses so that the user can best identify what to do next or where a problem could have arisen. More implementation methods of HCI include Command Line interfaces, so that when typing code, the user can communicate with the machine to navigate through text, and Menu Driven Interface.

HCI is responsible for creating an environment in which the user is comfortable using the machine, and can navigate without issue, otherwise they could end up irreparably damaging the software or the operating system. This is why HCI is so important, and why figuring out the best practices for how to properly implement the methods to improve user experience is crucial to developing a good software and improving security of everyday users. Understanding the principles of good design using Human-Computer Interaction is the first step to reducing human error in protecting secure information.

2. PRINCIPLES OF EFFECTIVE HUMAN COMPUTER INTERACTION

Due to the fact that there is no committee centered around the concept of HCI as there is for ethics with ACM or making specific programs universal, there is no universal set of principles. A lot of the implementation methods for HCI are completely abstract, and because of this, the rules for implementing resemble more guidelines. Despite this, there are plenty of HCI professionals who create their own set of principles where each can be combed through and compared to determine a set of principles that are nearly universal. While these sets can range from upwards of 10 to 12 principles, from these sets of alternate personal principles from HCI professionals, a set of five (5) common principles can be attributed as an encompassment of all the other principles.

2.1 Affordance

Affordance is the concept that when a feature or design on the interface is presented to the user, and the user can tell instantly what to do with it. Even if it can be used for a purpose other than what it was originally expressly designed for, as long as it is clear to the user and each of its functions are outlined in a way that can be determined by them, it follows this principle. This also means that whatever purposes that a feature can fulfill that work in conjunction with other features should also be visible and clearly available. Examples of affordance are labeling website or software navigation with the correct wording or symbols that most people would understand to be taking them to a specific aspect of a website or software. Using the logos of social media in a "Contact Us" or "About us" section can clearly show to the user that clicking on it would lead them to the creator's social media page. Labeling a search box with a magnifying glass helps differentiate the text box as a way to search the website rather than sending a message which could be labeled with an envelope to signify mail.

2.2 User Feedback and Interaction

This is by far the most important principle, as interacting with the user after they do something they should or shouldn't do is what HCI is put in its simplest form. This principle is very broad since there's so many ways that users need feedback to tell what they are doing on the machine. If the user has broken something, entered something that does not properly meet constraints of the website or software, or gone to a portion of the product that no longer or has never existed, they need the feedback of an error telling them that they've made a mistake. When the website or software needs time to load new or larger portions of itself, it should put an indicator onto the website such as a symbol of an hourglass, or outright placing "loading" or "waiting" on the screen so the user can be made aware and knows the website hasn't broken. This feedback allows the user to know what they should and shouldn't interact with or attempt to pursue further.

2.3 Setting Constraints

Just as important as letting the users know that they are on the right or wrong track, setting up preventative measures to prevent them from proceeding without proper security measures or keeping them from entering sections of the software or website in which they do not belong. Showing the user messages of error during moments in which they make mistakes or fail to meet the requirements of the software or website is important to making sure all features are used correctly as to prevent the software from breaking or as a means of keeping the user and their data safe in specific situations. An example of setting constraints within security would be password creation, and how over time, the constraints become progressively more rigorous, because if the machine did not inform the user of the poor strength password, their account could easily be accessed by a hacker with minimal skill. If there wasn't a password attempt limit, a dictionary hack could be performed, brute forcing the account with minimal guesses due to the limited number of characters, lack of variation in the characters, or easily guessable sequences of characters. This is also why another form of restraint is to limit the number of times a user can enter the password incorrectly before they become unable to access the account or need to reset the password.

2.4 User control and flexibility

Even if the user needs to be guided and constrained at certain points during their user experience, they should still be able to navigate and maneuver through it in a way that makes them comfortable and want to return. Once they bypass the security of the website that restricts access to features without an account, anything they want to do with their account is up to them, even if technically it's not always advantageous to them. If they are too constrained or lose too many features due to upped security, then they won't want to use the product on their machines. An example of such is anti-virus, where it completely blocks the download of certain programs and files onto the machine if it is deemed unsafe, but sometimes, it can deem files which the user knows is safe as unsafe, as it has come from a trusted source or is a file that they created or use regularly. These constraints could lead to someone outright disabling their antivirus.

2.5 Consistency

Consistency is about nothing more than following all the guidelines in a similar fashion throughout the entirety of the product made. If constraints change consistently, then users will not enjoy the product. If the way affordance works among various features on the application change regularly, then it will become difficult to navigate and manage for the user. This is not as complicated as many of the other principles, because it's about nothing more than not changing what works for the users, and making it work that way throughout the whole program so that each of the principles cannot go disregarded by the user.

3. ANALYSIS OF HCI IMPLEMENTATION IN CYBER SECURITY

3.1 Stress Levels from Error Analysis

It is a proven fact that displaying an error message to a user raises cortisol levels, increasing stress within an individual. However, levels of stress range from positive to negative amounts of stress.

Figure 1: An infographic on the effectiveness of stress as a motivator for performance, and the risk for the opposite effect.

User performance is empowered, by a moderated level of stress created by showing a stress inducing symbols or wording. Ways to increase the stress induced by these would be to stack these methods, such as using more bright red within the error message, using warning symbols such as stop signs or danger symbols, or using capitalization and exclamation points. However, extra stress can be caused through the frustration of poor error message design, causing higher cortisol levels and lower levels of user cooperation.

Figure 2: A list of words that create an increased negative reaction within users.

This set of words has been studied to induce a greater negative reaction in users that see them, increasing cortisol past the eustress levels to distress levels that make users not want to use a product. When these messages are used to demonstrate constraints or used in preventative measures in cyber security, there's a greater chance that they will go ignored and disregarded, or they will quit the application or website, which could lead to greater risk of security failure.

3.2 User Survey Data Presentation

A survey was conducted for this research paper, as a means of getting a better sense of ways in which poor HCI had resulted in breaks in security. A set of 5 questions pertaining to ways in which people who had problems with software or websites that deal with cyber security or more general purposes that could be attributed to potential issues in cyber security. A sample size of 60 people chosen randomly was used.

Demographical Data

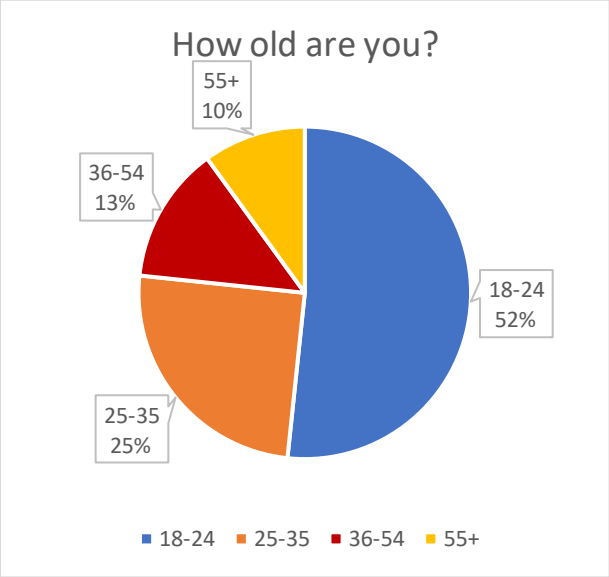


Figure 3: Participants by Age-Range.

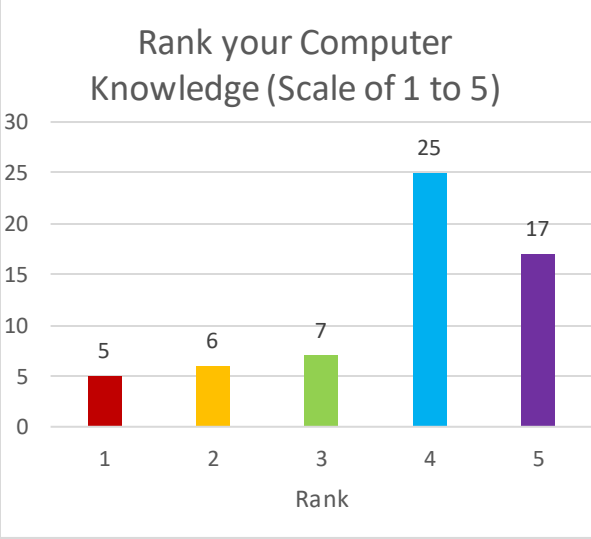
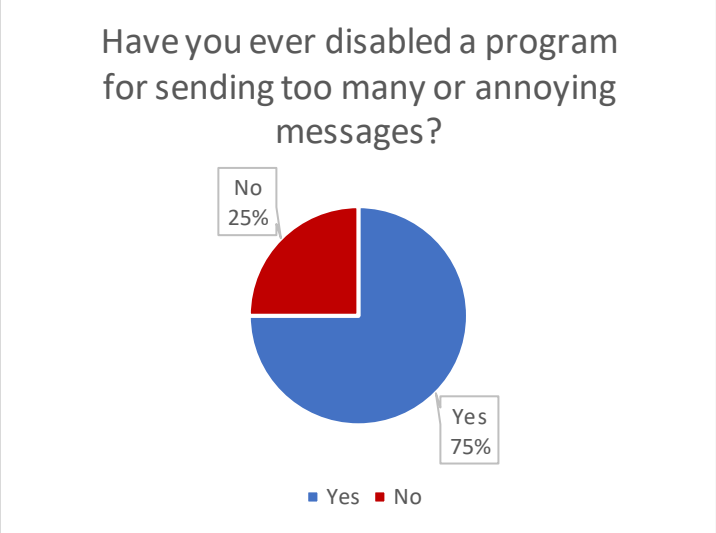
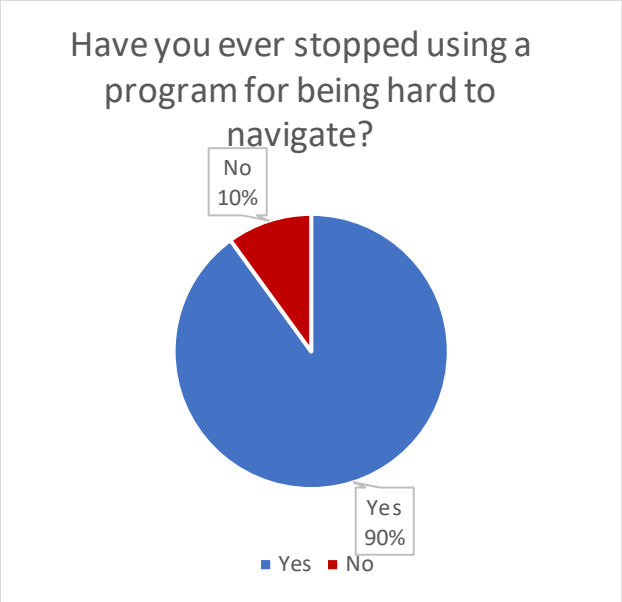
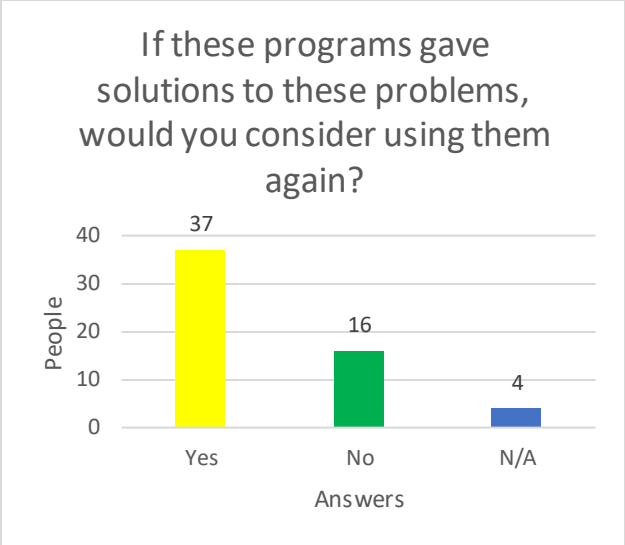


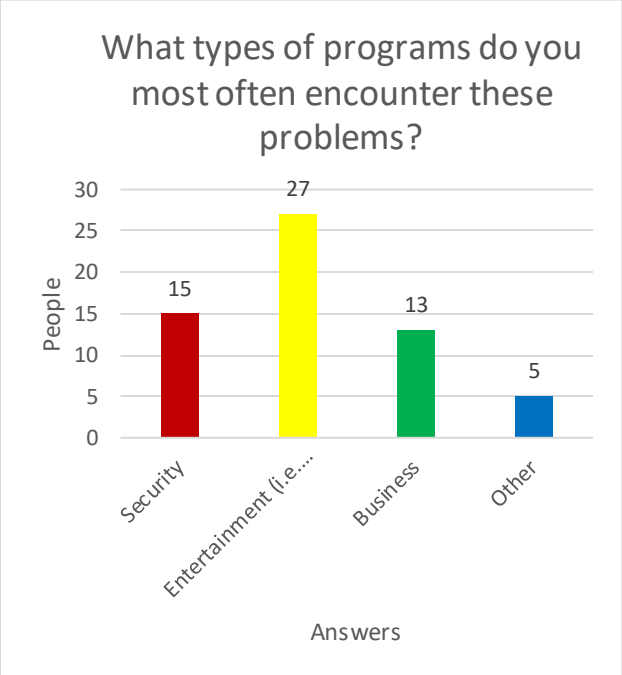
Figure 4: Participants by Computer Skill (1-novince to 5 skilled/expert).

Survey Data









Entertainment including games and music

3.3 Analysis of Result

It can be seen from the results taken from the survey that users can frequently experience issues with programs and websites, pertaining to HCI, ranging from lack of affordance to lack of freedom and control. It also shows that due to these, people would be willing to disable important security aspects about their computers just to prevent from having to see those messages or deal with poor Graphical User Interface design. When programs aren't designed correctly or aren't interacting with the user in a way that the user can agree with, they might be willing to put their entertainment, business, or their computer security at risk.

A more positive statistic that has been gleaned from the survey is that demonstrating constraints to the user at the expense of convenience is not actually a detriment to the user experience. This means that security will not always be sacrificed by the user for the sake of their freedom, and security does not need to be sacrificed by the developer for the sake of pleasing the user. Maintaining constraints does add to the user experience as the principles suggest but sending too many messages and thus not handling user interaction well, as well as not allowing some freedom to the user. A similar understanding can come from the lack of affordance given from poor design.

4. CONCLUSION

Taking all the results gathered from the process of the paper into account, it is clear that when considering personal security, risks can and will be taken to avoid the stress and inconvenience of poor Human-Computer interaction implementations that overwhelm and

restrict the users that are found within software programs and websites. While the aforementioned is true, more often than not, properly implemented HCI concepts that also restricts the user can lead to actually lead to better security while still leaving the user unbothered. HCI can take the form of a passive layout or an active message, but well executed HCI can do either in a manner without sacrificing the experience of the user. That is why cyber security programs that work with either the cyber security expert or the standard individual who simply needs to practice proper personal security, need to implement proper HCI. When security settings on a personal machine are center, easy to navigate and find, intuitive, and warn the user in a way that is not restrictive or condescending, the security of that user should increase. When a cyber security expert makes use of a program for their profession, and the HCI is not intuitive and responsive, then the ability to complete their work and motivation to continue working would logically decrease and affect the security of others. Computer science concepts such as cyber security and HCI both fall under the blanket of computer science, and therefore, more specializations under computer science should be taught and learned in conjunction.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award# 1754054.

References

Ambielli, B. (2018, August 6). 15 Principles for Human Centered Design. Retrieved from B Ambielli: 15 Principles for Human Centered Design

Birkett, A. (2019, July 23). Error Messages: Examples, Best Practices & Common Mistakes. Retrieved from CXL: https://cxl.com/blog/error-messages/

Caroll, J. M. (n.d.). Interaction Design Foundation. Retrieved from Interaction Design Web Site: https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/human-computer-interaction-brief-intro#:~:text=Human%2Dcomputer%20interaction%20(HCI),science%20and%20human%20factors%20engineering.

Hefferman, K. (2015, April 13). BAD ERROR MESSAGES ARE HARMING YOUR USERS - THE UX OF ERROR MESSAGES. Retrieved from Kayla Hefferman Website: https://www.kaylaheffernan.com/blog/2014/12/9/error-messages

Moallem, A. (2018). Human Computer Interaction adn Cyber Security Handbook.

Murphy, L. (2018, April 27). 5 DESIGN PRINCIPLES OF HUMAN COMPUTER INTERACTION. Retrieved February 2021, from http://www.lukemurphy.info/5-design-principles-of-human-computer-interaction/

Myers, B. A. (1999, October 28). Overview of HCI Design and Implementation. Retrieved 2 2021, from Carnegie Mellon University: https://www.cs.cmu.edu/~bam/uicourse/special/

Schneiderman, B. (2013, September 12). Shneiderman's "Eight Golden Rules of Interface Design". Retrieved February 2021, from Design Principles FTW: https://www.designprinciplesftw.com/collections/shneidermans-eight-golden-rules-of-interface-design

Tutorials Point Corporation. (n.d.). Guidelines in HCI. Retrieved from Tutorials Point: https://www.tutorialspoint.com/human_computer_interface/guidelines_in_hci.htm