iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** VII **Month of publication:** July 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.36246

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VII July 2021- Available at www.ijraset.com*

# HCI: Use in Cyber Security

Neelabh Kulshreshtha[1], Sunit Basak[2], Ms Monika[3]
[1, 2]*Department of Computer Science Engineering, Manav Rachna International Institute of Research and Studies Manav Rachna Campus Rd, Gadakhor Basti Village, Sector-43, Faridabad, Haryana 121004*
[3]*Assistant Professor, (Computer Science & Engg.) Faculty of Engineering & Technology, Manav Rachna International Institute of Research & Studies, Delhi Surajkund Road, Sector 43, Faridabad, Haryana 121004*

***Abstract: This paper deals with the uses of HCI (Human-Computer Interaction) with Cyber Security and Information Security. Even though there have been efforts to strengthen the infrastructure of the security systems, there are many endemic problems which still exist and are a major source of vulnerabilities. The paper also aims to bridge the gap between the end-user and the technology of HCI. There have been many widespread security problems from the perspective of the security community, many of which arise due to the bad interaction between humans and systems. Developing on the Human-Computer Interaction is an important part of the security system architecture because even the most secure systems exist to serve human users and carry out human-oriented processes, and are designed and built by humans. HCI is concerned with the user interfaces and how they can be improved because most users' perceptions are based on their experience with these interfaces. There has been immense research on this field and many advances have been made in this arena of HCI. Speaking of Information Security on the other hand has been a major concern for the present world scenario where everything is done in the digital world.***
***Keywords: HCI, human-computer interaction, Information security, Usability Trust Firewalls HCI-S***

## I. INTRODUCTION

HCI or Human-Computer Interaction is the study of the interaction of people with computers. This field also checks the extent computers are or aren't developed in order to have a successful human interaction.

As its name implies, HCI has three important parts:

*1)* The user,
*2)* The pc itself,
*3)* And therefore the ways they work together.

### *A. User*

The "user", means an individual person or a group of people or users who work together. It is very important for us to know how the people's sensory systems including the sight, hearing and touch relay information. This is important for HCI as well. Moreover, different users form different conceptions of mental models in accordance with the interaction of them and the computer which leads us to the fact that they have different ways of learning and implementing the knowledge. Also, there are many other differences which play an important role in the field, such as cultural and national differences.

### *B. Computer*

The term computer refers to a wide variety of desktop PCs, laptops and all other kinds of computer systems available including mobile phones and VCRs. Even when we discuss the design or the functioning of the website, then, in that case, the website would be treated as the computer.

### *C. Interaction*

There are obvious differences between humans and machines but still, HCI tries to bridge the gap and between the two and help them to interact well. In order to realize a usable system, you would like to use what you recognize about humans and computers and consult likely users throughout the planning process[3] In real systems, the schedule and therefore the budget is important, and it's vital to seek out a balance between what would be ideal for the users and what's feasible in reality.[4]

HCI Security aims to improve the usability of security features in end-user applications.

The HCI Security is indeed a developing field of study and this has been proved by comparison. Interest during this topic tracks thereupon of Internet security, which has become a neighbourhood of broad public concern only in very recent years.

©IJRASET: All Rights are Reserved

When security measures exhibit poor usability, the subsequent are common reasons:

1) they were added in casual afterthought
2) they were hastily patched in to deal with newly discovered security bugs
3) they address very complex use cases without the advantage of a software wizard
4) the interface designers might not understand the related security concepts or might lack the knowledge of it.
5) their interface designers weren't usability experts (often meaning they were the appliance developers themselves)[5]

## II. THE GOALS OF HCI

The goals of HCI are to supply usable and safe systems, also as functional systems. In order to supply computer systems with good usability, developers must attempt to:

1) have the knowledge of the factors which determines how people use technology
2) developing tools and techniques which enable the building of suitable systems
3) aim to get efficient, effective andsafe interaction
4) put people first

The theme of HCI is dependent on the belief that the people using a computer system must always come first. The designers should look for all the possible needs, capabilities and preferences of performing various tasks while they make the software, It must not be the people who must adjust to the system rather the system should be the one which must change according to the needs. It should be designed in that manner.[6]

## III. USABILITY

Usability is one of the key concepts in HCI. It is concerned with making systems easy to learn and use. A usable system is:

1) easy to learn
2) easy to remember how to use
3) effective to use
4) efficient to use
5) safe to use
6) enjoyable to use

### A. *Why is usability important?*

Many everyday systems and products seem to be designed with little regard for usability. This leads to frustration, wasted time and errors.

### B. *This List Contains Examples Of Interactive Products*

Mobile phone, computer, personal organizer, remote control, soft drink machine, coffee machine, ATM, ticket machine, library information system, the web, photocopier, watch, printer, stereo, calculator, video game etc.

How many are actually easy, effortless, and enjoyable to use?

For example, a photocopier might have buttons like these on its control panel.

Imagine that you just put your document into the photocopier and set the photocopier to make 15 copies, sorted and stapled. Then you push the big button with the "C" to start making your copies.

### C. *What do you think will happen?*

1) The photocopier makes the copies correctly.
2) The photocopier settings are cleared and no copies are made.

If you selected (b) you are right! The "C" stands for clear, not copy. The copy button is actually the button on the left with the "line in a diamond" symbol. This symbol is widely used on photocopiers, but is of little help to someone who is unfamiliar with this.

©IJRASET: All Rights are Reserved

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VII July 2021- Available at www.ijraset.com*

## IV. INFORMATION SECURITY

Information Security is treated in five services: Integrity, Non-Rejection, Authorization, Confidentiality, Identification and Authentication. These services are necessary to ensure that the data is safe and secure. Identification and authentication is the first step in implementing security.

Authorization is the next step in deciding whether the confirmed case has the right to access the affected computing facilities. All materials must be strictly accessible to authorized users.

Confidentiality means that only authorized parties can access the information. Confidentiality is necessary, but integrity must also be guaranteed. Therefore, only the authorized user can change the content.

Non-rejection means that no change to the content can compromise the security of the information. These services must be accessible, visible and functional from the point of view of human-machine interaction in order to receive information Safety.

## V. HCI FOR INFORMATION SECURITY TECHNOLOGY

Employees are responsible for security problems that cause failures in the computer system. It is possible to advance or improve the execution of information security taking into account certain aspects. First, understand the problem that comes with providing secure interaction. The following complexity reduces security. Information security is only guaranteed if all functions are visible to the user and he knows how to use them [1].

### *A. HCI-S Guidelines*

Here are some HCI rules that the presentation must follow in order to get the correct HCI properties. Ten key models were trained and the applications for each estimated.

Status of notable organizational and security goals:

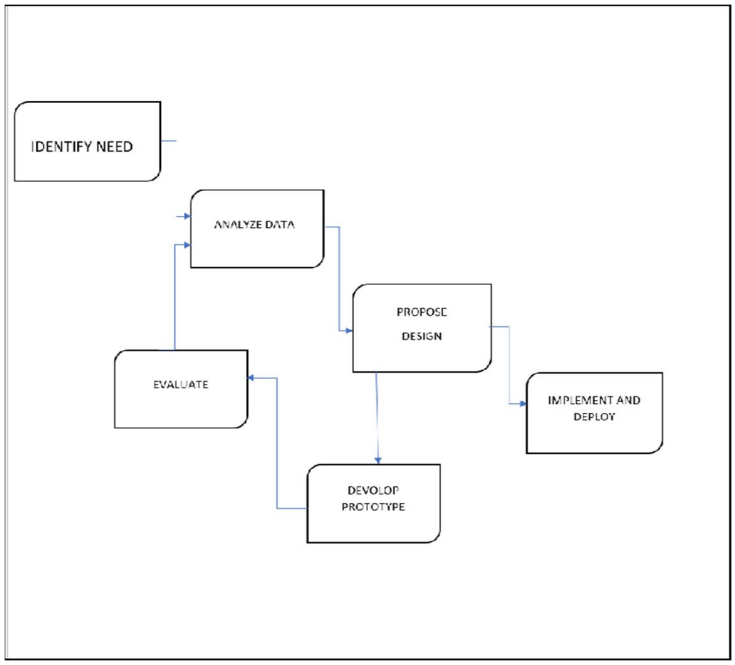
All security-related functions should be visible to the user. You shouldn't have to search for them for the changes to take effect. The system should always keep customers up to date on the latest developments through appropriate feedback within a reasonable time frame [1]. Most of the time, the current security status display can be used to provide customers with thoughtful information about data security. Visibility of the security state of the system contributes to the operation is trusted and therefore sets the standard for an efficient human-machine connection in safety applications.Security should be visible without being intrusive, as customers prefer documents, dynamic symbols when security capabilities are running on a system.

1) *Security Should Be Easy To Use:* The user interface should be designed so that the use of security features requires less effort. The interface must be put together carefully and requires negligible rendering effort. Use of security fortresses. In addition, security settings should not be set in a few separate areas of the application as it is difficult for the customer to find all the settings.
2) *Suitable For Novice And Advanced Users:* The apps are designed for both new and experienced users. So show enough information for an experienced user and detailed information for a new user. There should be both shortcuts and defined methods for each application role so that new users can use well-defined methods. Get the job done and power users can use shortcuts. It can be easy to use and there should be a shortcut available for advanced users.
3) *Avoid Using Too Much Technical Vocabulary Or Advanced Terms:* Many application users may not have a good command of the language or vocabulary. If the designer is using a function that has difficult vocabulary, the user will surely be confused about which function to choose The corresponding function according to your requirements. So use simple words and vocabulary to avoid misunderstandings.
4) *Treat Errors Appropriately:* Good error messages are a questionable interaction design that prevents a problem from occurring in the first place. Therefore the system should not contain any errors- Articles are and should be avoided for possible user errors. Errors caused by using the safety function can be forbidden and minimized.
5) *Allow Customization Without The Risk Of Being Scammed:* New and old users are sometimes unaware of the proper functionality of certain features. The exit path must be available if a function has been selected by mistake. If the user makes a bad choice and does not exit immediately, he will not be aware of this using any security function until then. The need for an exit path is necessary. *Example:* In many applications, there is a back key or when we press the Esc key or On the keyboard, we are outside of this particular area.
6) *Easy Configuration Of Security Settings:* Security settings are a basic need of the user. To implement security according to customer requirements, all available parameters must be easily understandable and visible, and the vocabulary must be easy to understand. It should be easy for everyone to adjust the settings to suit their needs.

©IJRASET: All Rights are Reserved

7) *Adequate Security Support And Documentation Available:* New users should receive support and documentation. Offer your customers quick access to support resources. Organize help around your tasks and goals. Provide complete and precise help. Write what is appropriate in the documents.
8) *Make Users Feel Protected:* Make sure the user protects their work through the app. Recovery from sudden failure should be considered and the application should ensure that clients do not lose their information. Applications should provide the most up-to-date security to the client, including a specific end goal to feel safe. Also, some sort of notice would be helpful if there is a possibility that a security update is available.
9) *Security Should Not Affect Performance:* If we increase security, it means usability decreases and as usability increases, security decreases. So, improve the security features, but also consider the performance by using efficient algorithms.

Flowchart




*credits: tutorialspoint.com* [7]

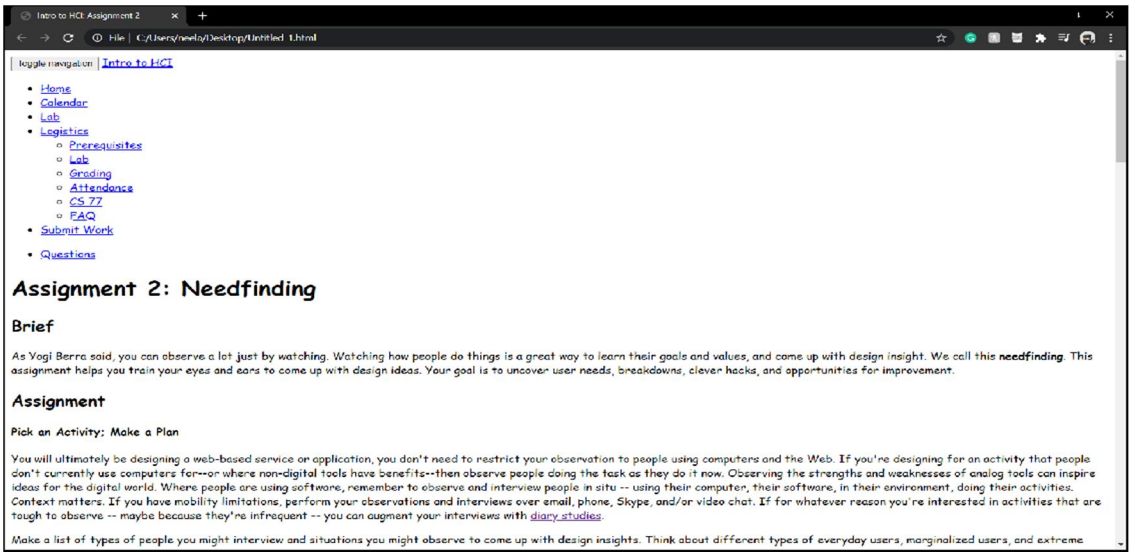



Fig: this is a sample website in which we will see how the computer react when there is no malware present in any of the given links.

©IJRASET: All Rights are Reserved

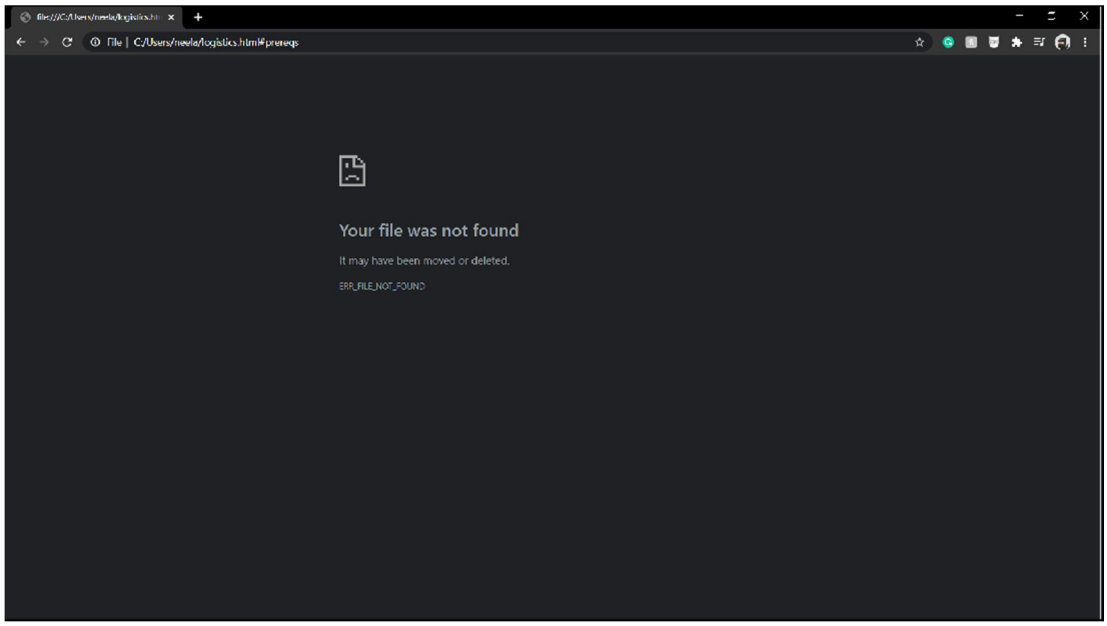
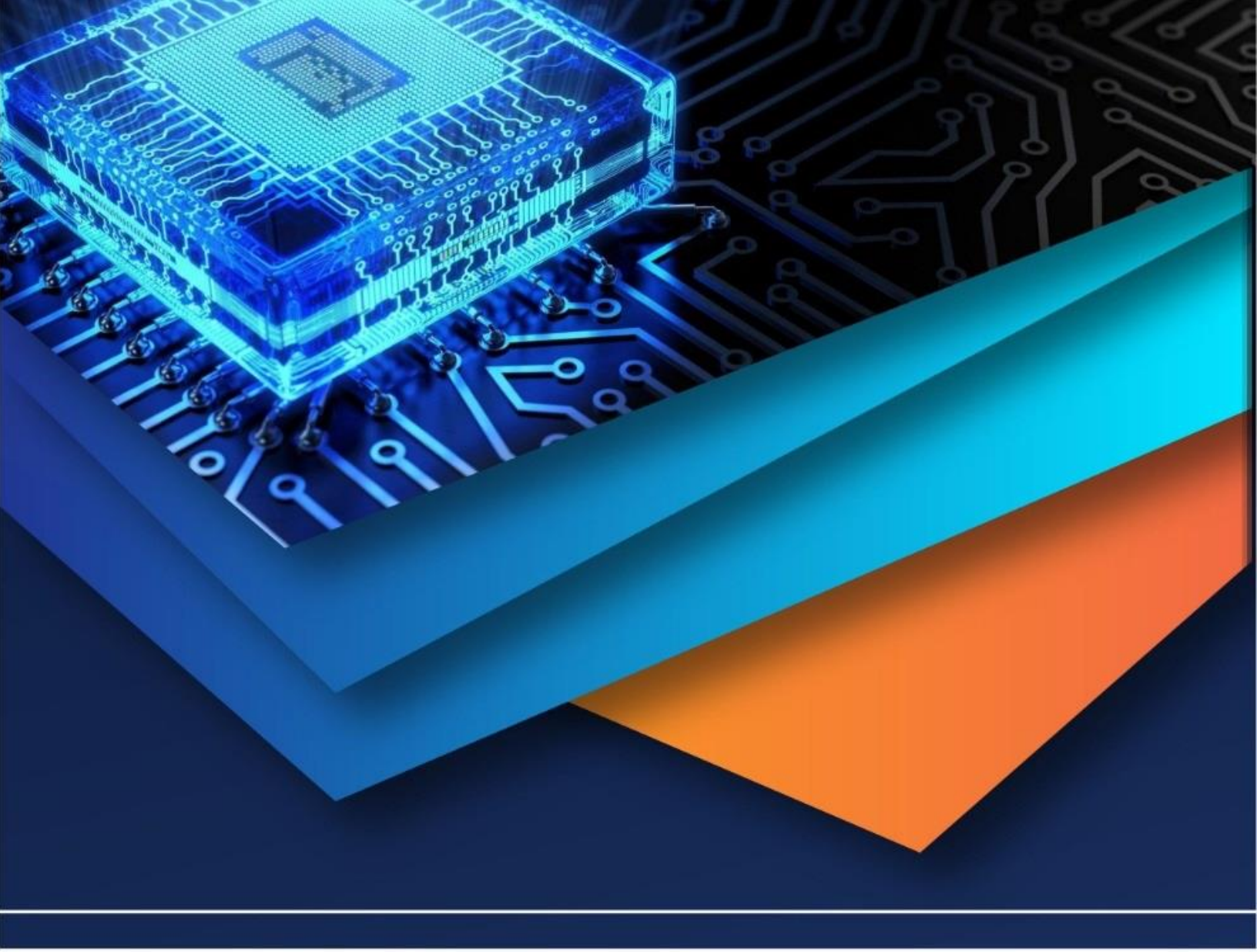



Fig: so in the figure as you can see there is no popup about whether the link contains any malware so this means that the link was safe (Normally in any published website in the link https i.e. hypertext transfer protocol is used which tells us that the network is secure)

## REFERENCE

[1] M.M. ELOFF, J.H.P. ELOFF. "HUMAN COMPUTER INTERACTION: AN INFORMATION SECURITY PERSPECTIVES." RAU Standard Bank Academy for Information Technology Rand Afrikaans University, Johannesburg, South Africa.
[2] Hussain Mohammad Abu Dalbouh. "Implementing End-User Privacy through Human Computer Interaction for Improving Quality of Personalized Web." Computer and Information Science; Vol. 9, No. 1; 2016.
[3] https://www.cs.bham.ac.uk/~rxb/Teaching/HCI%2 0II/intro.html
[4] https://www.coursehero.com/file/p7eo0am/In-real- systems-the-schedule-and-the-budget-are-important-a nd-it-is-vital-to/
[5] https://en.wikipedia.org/wiki/Human%E2%80%93 computer_interaction_(security)
[6] https://www.google.com/url?q=https://shodhganga .inflibnet.ac.in/bitstream/10603/13990/6/06_chapter_ 1.pdf&sa=D&ust=1602592013871000&usg=AFQjC NF_HvMb8xitysaM8Xg3GY15o2T54w
[7] https://www.tutorialspoint.com/human_computer_ interface/quick_guide.htm

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)