Seminar 2

In the domain of information security, there is an adage that states, "If customers had to pick between dancing pigs and security, they would always go for dancing pigs." However, this is an inaccurate generalization; neuroscientific research reveals that the seemingly irresponsible security behavior of users is really the product of how the brain operates (Vance, A. 2017).

Usable security action has lot dependence on user security decision. Sometimes it can say that human, human brain and behaviour is the weakest link the chain. There are many factors which are involved in implications of human brain in usability security design (Hartson, & Pyla, 2019). Some of them are presented below:

1. **Dual-task Interference:** It is the state that occurs when numerous tasks are being carried out at the same time, which causes interference in the brain. For example, if a user is looking at something that has an interested and appealing UI, and at the same time there is a security popup that appears in another window while they are doing this, the user will ignore the security popup and will focus on their movie, drama or a game. This indicates that the user's brain is more dependent on and attracted to items that have a decent interface and are interesting rather than those that are secure.

**How to overcome:**

1. The brain isn’t good at handling interruptions so train your brains according to security designs.
2. Timing a security message to display at a low-DTI results in marked improvements
3. **Habituation:** The process of habituation is a kind of non-associative learning in which an innate response to a stimulus becomes less visible following prolonged or repeated exposure to that stimulus. Responses that may become habitual include both those involving the whole organism and those involving just sections of the organism (Wikipedia C., 2019).

**How to overcome:**

1. Updating the security UI can reduce the habitation Process.
2. The human brain is wired to tune out things it has seen before, so train accordingly.
3. **Generalization:** This describes situation in which you become heavily habituated to one stimulus and then you can encounter one stimulus and that habituation carries over because two stimuli share visual similarity (Generalization. 2021).

**How to overcome:**

1. Design security messages to be visually distinct
2. Frequent notification likely contributes to habituation to rare security messages.

Even though other researchers have looked at usable security design, the work that Kai-Ping Yee did in 2002 is still widely recognized as being among the best (Yee, K.-P. 2002). His proposals focus on valid and nontrivial problems peculiar to usable security design. All are described below:

1. **Least Resistance Path:** Find the most effortless way to do tasks that demands the least amount of effort from you.
2. **Authorization:** that is currently in effect. It is acceptable to assign authority to other parties based on user actions that show consent.
3. **Revocability:** Provide the user with alternatives to restrict the access of others to his or her resources.
4. **Visibility:** Maintain an accurate understanding of the authority possessed by others, especially as it pertains to user preferences.
5. **Self-awareness:** Always maintain an accurate knowledge of the user’s own authorization to access resources.
6. **Trusted Path:** The dependable route Protect the user's access to the agents who will act on their behalf and manipulate power.
7. **Expressiveness:** Make it easy for the user to express security rules in a manner that is specific to their activities.
8. **Relevant Boundaries:** Make differences between the objects and actions you do along the work's critical boundaries.
9. **Identifiability**: Utilize unique and realistic appearances to illustrate the actions and objects you're addressing.
10. **Foresight:** It is essential that the consequences of the decisions the user is expected to make be made crystal clear.

According to Garfinkel, there is no set of rules, principles, or formalisms that, when followed, guarantees the production of usable computer systems. If such restrictions were in place, it is quite probable that we would all adhere to them, so resolving the problem with usability. 16 However, even though these standards do not address and give a solution for every issue, they may be useful for highlighting best practices to designers. They may be helpful in this respect.

**References:**

Vance, A. (2017). What Does the Brain Tell Us about Usable Security? Www.usenix.org. Retrieved from <https://www.usenix.org/conference/enigma2017/conference-program/presentation/vance>.

H Rex Hartson, & Pyla, P. S. (2019). The UX book : Agile UX design for a quality user experience. Cambridge, Ma: Morgan Kaufmann.

Yee, K.-P. (2002). User Interaction Design for Secure Systems. Information and Communications Security, 278–290. <https://doi.org/10.1007/3-540-36159-6_24>

Payne, B. D., & Edwards, W. K. (2008). A Brief Introduction to Usable Security. IEEE Internet Computing, 12(3), 13–21. https://doi.org/10.1109/mic.2008.50

Wikipedia Contributors. (2019, September 20). Habituation. Retrieved from Wikipedia website: https://en.wikipedia.org/wiki/Habituation

Generalization. (2021, January 8). Retrieved from Wikipedia website: https://en.wikipedia.org/wiki/Generalization