NO SECURITY WITHOUT TRUST

security-by-design.net

A First Step Guide for Interface & User Experience Designers by Thomas Otto

MORE SECURITY BY DESIGN

Security in User Interface Design? How should this happen? Aren't these business or «Code Decisions»? Something within hardware, code inside our applications, new «Business Models» or something that an update will fix? Wrong. Every new service we create, every new interface we are working on has consequences depending on our decisions. If designers don't ask questions like «Why do we need this data?» or «Should we tell the user what we do?», nobody will. It will go final and in worst case live and people will use it.

That this kind of «Irresponsible Design» is happening is shown by several examples and great talks like «How Designers Destroyed the World» by Mike Monteiro.

So keep the Testimonials and Steps in mind when you create new amazing things.

PROJECT INFORMATION

The project is a result of the course «Designing for Trust and Security» by Prof. Frank Heidmann and Andreas Thom (MA), developed in winter semester 2014.

Served as the main basis are the security guidelines from the book «Security and Usability- Designing Secure Systems that People Can Use» by Lorrie Faith Cranor and Simson Garfinkel.

12 TRUST TESTIMONIALS

«The Trust Testimonials»: Easy steps to give you a basic understanding what you can do to influence users to give your idea a try.

Create attractive Design

«Aesthetics is the ›immediate pleasurable subjective experience that is directed toward an object‹» [1] [2]

For a professional perception, avoid simple mistakes

«One of the key findings is that trust seems to be related to beliefs about another's ability, integrity, and benevolence.» [3]

Include background information such as indicators of expertise

Who is offering the service or application? What expertise or which experts do you have? [3]

Separate content and advertising clearly from each other

«[...] advertising had the most negative effect on participants' judgement [...]» [2]

Maximize consistency

Keep familiar interactions in mind. If you create new ones, make them predictable visually and in terms of process.

«[...]Merriam-Webster says, that consistency is the "agreement or harmony of parts or features to one another or a whole."[...]» [4]

Offer explanations and detailed information

Tell your users why you need certain data for your service/application. Don't hide information of use to them. [3]

Communicate Security Technologies

Communicate to your users which technologies you are using to protect them. Explain why, if they affect the usage of your service/application.

Provide independent space of your users opinions and give them the opportunity to contact you

«Reading about the experiences and opinions of other users in forums seemed to enhance trustworthiness.» [2]

Provide clear security and privacy statements

Clearly explain what user data you use and why you use it.

Clarify Responsibilities

Who is behind the service/application? Who can help if necessary?

Ensure communication remains open and responsive

Make sure there are enough contact options. Don't hide behind a confused information structure.

Request only the data you actually need

Ask users for permission to use their data or ask them to fill out forms. Just take what you really need. [5]

6 BASIC SECURITY STEPS

Users trusting you with their data is what lets your idea become alive. «Security Steps» will give you a golden thread to create a more secure environment for your users.

Identify the security needs.

Who is your audience and which security levels are needed? These are questions that you should keep in mind by creating a flexible security model. [3]

Explain the importance of data security to the users.

«[...]And yet, the security indicators as special type of security usability features are of no value when the users do not know how to rank them.» [2]

Security that is easy to use is good security.

«Security is dependable only if it is actually used as intended.» [3]

Be aware of the goals of the user (based on context).

«Insufficient communication with users produces a lack of a user-centered design in security mechanisms. Many of these mechanisms create overheads for users, or require unworkable user behavior.» [6]

Trust users and treat them as intellectual individuals – individuals make mistakes.

«[...]fundamental requirement is simply that software provides its users with accurate information for risk assessment.» [7]

Don't punish users. Reward them for acting secure.

«There is no feedback on good security behaviour; it is rewarded only by the non-occurrence of security incidents.» [2]

SOURCES

1 **«Facets of visual aesthetics»**
Morten Moshagen, Meinald T. Thielsch, 2010

2 **«Human-Computer Interaction and Online Users' Trust»**
Nina Bär, 2014

3 **«Security and Usability- Designing Secure Systems that People Can Use»**
Lorrie Faith Cranor, Simson Garfinkel, 2010

4 **«Designed for Use - Create Usable Interfaces for Applications and the Web»**
Lukas Mathis, 2011

5 **«From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interfaces»**
Andrew S. Patrick, Steve Kenny, 2003

6 **«COMMUNICATIONS OF THE ACM - Users are not the Enemy»**
Anne Adams, Martina Angela Sasse, 2014

7 **«Making Security Usable»**
Alma Whitten, May 2010