**Login on Smartphones: A Triviality?**

Johannes Volk, Federal Statistical Office of Germany, johannes.volk@destatis.de

Karen Blanke, Federal Statistical Office of Germany; karen.blanke@destatis.de

**Abstract**

*There is ongoing discussion about transforming online questionnaires into an appropriate mobile device design in order to avoid mode-effects and safeguard data quality. However, a crucial point in implementing online questionnaires is often neglected or less discussed: The dropout rates of potential participants due to problems in accessing the online instrument caused by a faulty or inconvenient login process.*

*In our qualitative study, concrete evidence on the design of an easy login on Smartphones could be iteratively developed to meet users’ requirements.* *Results suggest using catchy passwords, displaying passwords rather than fading them and implementing proportional fonts rather than non-proportional. Moreover, we analysed the duration of the login process, the layouts of different keyboards, the design of input fields, the layout of the login information in the invitation letter and the subjective ratings of lead probands on subjective efforts and security issues. In the end, we developed a combination of login design elements, which better suit the user’s perspective. However, further investigation on data security requirement is needed before a new design can be implemented.*

**Keywords:** Smartphone design, online data collection tools; login process, passwords

**1. Introduction**

As times have changed and digitalisation has become not only a buzzword but reality, more and more surveys are conducted online as computer assisted web interviewing (CAWI), mainly on PCs and laptops. In addition, while online surveys are also increasingly being implemented in official statistics, Internet access is often performed via mobile devices and thus it is a reasonable claim to make data collection via mobile devices feasible. Consequently, the challenge for survey methodologists is not only to provide survey modes online and possibly in a mixed-mode design, but also to provide adequate survey designs and questionnaire designs which ensure data quality also on mobile devices (mixed-devices design). While general layout and design approaches are frequently discussed, the access to the online questionnaire is often neglected. One reason for this might be that many commercial and scientific surveys are carried out by huge online-panels nowadays. These circumstances differ from those in official statistics: Sampling frames and registers lack email addresses so personalised access is impossible from the beginning. Each time a new survey is introduced, the respondents need to follow login procedures.

In Germany, the initial contact to a respondent is via an invitation letter in the post, where instructions are provided as to how to access the website and login. As this first step seems to be crucial for every participant, we tested the login process on mobile devices.

The questionnaire of reference will be part of the Census 2021, where information on buildings and housing are collected. Participation is mandatory. Additionally, an Online-First-Strategy will be applied and presumably a high percentage may participate in the survey via a mobile device in 2021. Approximately 20 million respondents will participate in total. Even if only 5 % of participants would join via mobile device, this would result in one million persons having access by this mode. Therefore, the need for a more user-friendly login process on mobile devices is the ultimate goal and testing was initiated.

This paper will summarize the main findings of the study. Some parts will be described in more detail, while other results are disregarded, due to the entire length of the paper. However, in the conclusion, comprehensive recommendations are made.

**2. Methodology**

The qualitative study involved 27 probands, invited in an iterative setting of four waves to develop and test step by step an appropriate design. These probands came to our pretest laboratory and were asked to complete the survey on their own devices. After a short introduction, probands were left alone in the laboratory to enter data. The process was audio-visually recorded. Afterwards a cognitive interview was carried out. Further analyses based on the recording of the data entry process gave more insights. Probands covered all age groups, equally representing males and females. The devices used to participate in the survey included Smartphones (19) and Tablets (8), produced by different manufacturers and employed different browsers.

**3. Results**

*3.1. Access to Website*

Access via Browser

The first challenge appeared to be for probands to identify the URL in the invitation letter and open the correct website. Some probands did not type in the URL in a browser but started a search and got a hit list. While applying the hit list or typing in the URL, 7 probands had problems accessing the correct website. This result was surprising as the URL was rather easy in spelling, wording and length.

During the interview, we asked our probands to rate the access to the website. Even if the access to the website was not complicated and similar to a normal search for a website, four probands announced difficulties, even though the pretest laboratory setting may make people to be overly confident of themselves or unwilling to admit their insecurities.

**Figure 1. Self-Reported Effort to Access Website**



From these observations and feedback from the respondents, we learned that this short procedure which seemed to be rather easy might actually be problematic for a number of persons. Especially search results (for example with misspelled words) have to be improved and the correct website has to be better recognised and placed at the beginning of a possible hit list.

Access via QR Code

In addition to the “traditional” way of loading the website, the URL of the website was integrated in a QR Code and provided in the invitation letter. This made it easier and faster to access the page and login. The prerequisite for this was of course that persons (a) knew the procedure, (b) had installed a QR Code reader app, (c) perceived the QR Code and (d) wanted to use it.

Out of the 27 probands, only three scanned the QR Code to access the login page. Three other persons would have used the code if they had not overlooked it or had the corresponding app. However, those who applied the QR code access method were able to start the questionnaire quicker (see section on login duration).

Even though less common at the moment, this option should not be discarded prematurely. We therefore want to monitor the development and consider the possibility of using QR Codes in future planning.

*3.2. Login Information*

The login data consists of two codes: the access number (to call up the specific survey) and an activation code (to obtain individual access). Both codes were provided in the invitation letter.

**Figure 2. Login Information: Access Number and Activation Code**



Due to our findings, there is a risk that the codes will be mixed up, if the design and codes are similar. Consequently, for each code a specific design is recommended (see Figure 2): The access number in numerals and boxes in contrast to the activation code by applying alphanumeric symbols. Moreover, both login keys should be labelled as differently as possible. We recommend to use clearly distinguishable, common names for the login data, in which each word component (e.g. “number”, “code”, “activation”) occurs only once. For the design of the access number, there was a clear opinion in our test: three boxes with four digits each, separated by hyphens. In addition, the cursor automatically moved to the next input field as soon as 4 digits were entered in the first one. Both of these features were positively received by our test persons in the interviews.

Furthermore, the access number and activation code should not only have exactly the same name in the invitation letter and on the website but should also have the same form and be displayed in the same font. Concerning the input of the activation code, a numeric keypad should open to enter the digits. Further challenges on the activation code is presented in the next section.

*3.3. Design of Activation Code*

Another goal was to test the design of the activation code. Thirteen out of 27 test persons received cryptic activation codes, the remaining 14 persons received “catchy” ones. Since further results refer to these two groups, the differences between the two codes are presented in Figure 3. Basically, catchy codes are alphanumeric combinations by words, syllables and numbers, whereas the cryptic code applies non readable combinations.

**Figure 3. Cryptic and Catchy Activation Codes**



Login Problems

Eight out of the 27 probands did not enter the activation code correctly at the first attempt. Typical mistakes were typing errors caused by switching between lower case letters and capitals, no differentiation between lower case letters and capitals and overlooking of single characters. As the following evaluation shows, the results indicate that respondents with catchy activation codes make fewer mistakes.

**Figure 4. Login Problems**



Login Duration

To get a better impression of the duration of the login process, we analysed the time period in seconds. Here we report the median times for both groups.

**Figure 5. Login Duration**



Persons with catchy codes needed less time than test persons with cryptic codes. Persons who called up the login page via QR Code took a little less time to login than the respective median. The shorter time for QR Code users is no surprise since the participants didn't have to manually enter the access number, as it was preassigned with the QR Code.

Self-Reported Login Effort

In the cognitive interview, test persons who entered cryptic codes describe the change between the keyboard mappings (upper and lower case, digits, special characters) as complex, cumbersome and difficult. Of those with catchy activation codes, 6 persons positively emphasized that word components were used, which made it easier. In addition, we asked a closed question about their effort. The results support catchy codes (Figure 6).

**Figure 6. Self-Reported Login Effort**



In conclusion, objective indicators (number of login problems, login duration) and subjective indicators (self-reported login effort) suggest that catchy codes are preferred. The catchy activation code should consist of a total of 16 characters with memorable syllables or parts of words. It should combine lower and upper case letters together with numbers and 2 common punctuation marks. It should not start with a special character. Only the first letters of the syllables or parts of words should be capitalized. It should be displayed in a proportional font.

However, data security might make it necessary to rather use cryptic codes. This issue will be checked profoundly again.

**4. Concluding Recommendations**

Even though these findings are based on low case qualitative testing, the results provided important insights into the world of the respondents: There are several small details which are important to create a good login process.

*4.1. Invitation Letter*

We recommend a well-designed invitation letter, with...

* clear structure and subheadings
* clearly highlighted user credentials
* fonts and labels exactly as on the login page
* a pictogram showing that mobile devices can also be used

*4.2. Access to the Website*

* Access to the correct Login Page/Website is not trivial and should not be underestimated.
* Search engines should deliver the right Webpage for various search terms (including spelling and typing errors).
* In the hit lists of search engines, the correct page should be as high up as possible and easily identifiable.
* A QR Code supports error-free and easy page access. In addition, the preassigned access number makes it easier to log in.
* The prerequisites for the use of QR Codes are not yet optimal. The distribution and development of QR Codes and QR Code readers should therefore be observed. So far, it is recommended to keep the option open (to print a QR Code on the letter).

*4.3. Login to the Questionnaire*

* The two login codes (access and activation) should be designed and labelled very differently.
* It is recommended to use clearly distinguishable, common names for the login data, in which the word components occur only once (e.g. access number and activation code).
* The design of the access number was clearly defined in the test: three fields with four digits each, separated by a hyphen.
* If catchy activation codes are applied, they should be displayed in a long input field (see activation code). Separators and empty spaces should be technically ignored or blocked (with an error message).
* In the invitation letter, care must be taken to display the login data exactly as it appears in the electronic instrument (name, design, font).
* While catchy activation codes are preferred by respondents, data security regulations might be too restrictive to allow. There is no decision so far if catchy codes can be applied and legal examination has been initiated.
* We recommend a correction procedure in which the characters entered remain when the input field is clicked again and the characters to be corrected must be selected.
* The input should be open in plain text (and not hidden with black circles).
* A numeric keypad should be displayed as standard for entering numbers.

In summary, we identified many different details which can be addressed to simplify login processes systematically. In conclusion, Charles Eames’ word is even true for the design of login processes: “The details are not the details. They make the design.”