# Transaction Authentication
# 'Something you understand'
# The new factor in online security

Peter Gullberg
Gemalto eBanking
Gothenburg, Sweden, email: peter.gullberg@gemalto.com

## Abstract

Online attacks have advanced significantly in recent years. Two-factor authentication, which is used to protect online banking users, has not evolved at the same pace, meaning that users are not sufficiently protected against these new and advanced attacks.

This raises an important question: is it possible to make online activities more secure for the user? More specifically, we want to understand whether it is possible to prevent online attacks by involving the user? In this paper, we elaborate principles for providing security in factor-based authentication. We propose a strategy using these principles to make online activities more secure.

This paper introduces *Transaction Authentication* – the new factor for factor-based authentication – as a way to establish informed consent in the authentication and authorisation process for online security. We show how the solution provides security while minimising user involvement, by balancing security and usability.

## Categories and Subject Descriptors

H.1.2 [**MODELS AND PRINCIPLES**]: User/Machine Systems – *Human factors, Human information processing*

K.4.4 [**COMPUTERS AND SOCIETY**]: Electronic Commerce – Security

K.6.5 [**MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS**]: Security and Protection – *Authentication*

D.4.6 [**OPERATING SYSTEMS**]: Security and Protection (K.6.5) – *Authentication, Cryptographic controls, Invasive software*

## General Terms

Active participation, risk based authentication, dynamic signatures, transaction data signing, consent-based authorisation, informed consent, EMV, CAP, Chip Authentication Program, two-factor authentication, transaction authentication, context, usability, something you understand

## 1. Introduction

Most online banks are unable to protect their users from the surge in new and sophisticated online attacks. These come from underground networks with the purpose of making financial profit. Massive-scale online attacks against banks were uncommon before 2004, but have now become an industry.

The security solutions banks are using range from static passwords to more advanced one-time password or challenge-response solutions. While two-factor authentication is a common solution for protecting online banking users, there have not been any significant advances in the field of two-factor authentication since banks started deploying such solutions.

The sophistication of these new attacks has led to the failure of existing two-factor authentication technology, where the technology is no longer able to protect users. Drimer et al. [11] describe in their recent paper some of the vulnerabilities in two-factor authentication, as implemented by APACS in the UK.

Tygar and Whitten [1] in their paper show how to make a Trojan that executes in the browser using Java, referred to as 'Man-in-the-Browser' attacks. The attacks we see online are mainly phishing, Trojans, 'Man-in-the-Middle' and 'Man-in-the-Browser' attacks.

In this paper, we elaborate principles for providing security in factor-based authentication. We propose a strategy using these principles to make online activities more secure. We also want to understand if it is possible to prevent online attacks by involving the user.

We propose a concept, Dynamic Signatures, that integrates the elaborated principles and presents a new factor in online security, *Transaction Authentication* as a way to establish informed consent in the authentication and authorisation process. By involving the user, the process is visible and enables the user to give his/her informed consent to a transaction. We minimise the user's involvement by making a trade-off between security and usability, based on the risk in the transaction.

There are a few practical implementations based on this research that integrate context and user involvement in factor-based authentication.

## 2. Theoretical principles

In this section, we relate the principles that make a security solution usable. The section covers the principles of security, behavioural psychology, and cognitive science. All these principles need to be integrated into one solution working in concert, where each principle has its own importance, in order for the solution to fulfil its purpose. Used alone, however, any one of these principles will fail to protect the user against the sophisticated attacks we now see online.

### 2.1 User awareness

*'User awareness is the user's understanding of a process that he/she is performing'*; that he/she is partaking in. It also concerns their awareness of why he/she is performing the process, and their knowledge of how to complete the process. This is what establishes the level of user awareness.

Hertzum et al. [7] describe user awareness as when the user is able to understand why and how to complete the process. Failing to

understand why and how may weaken security. In order to provide user awareness, context is essential. Dey [13] provides a definition of context: *'A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task.'*

To achieve high user awareness with a security solution, the process should add context and be clear and easy to use. It is essential that, without further instructions, the user can understand the added context unambiguously.

User awareness can be established in several ways. One of the most straightforward ways is by adding descriptive texts that inform the user what he/she is doing, introducing context to the process.

Well-designed products increase user awareness by removing the stress, which is also described by Degani et al. [2]. Simplifying the user process reduces the cognitive load for the user, resulting in reduced stress.

When designing a product, the following aspects reduce the stress for the user; a feeling of trust, readability and hiding technical complexity. This also increases user awareness. With a low stress level, the user can use his/her mental capacity to focus on the context provided by the process. In a sense, this partially automates the user's task. These are also known as routine cognitive skills that enable the user to perform routine activities with a low cognitive load.

When needed, to increase a user's awareness, the use of an emotional message strengthens the user's conveyed intention and raises his/her attention [3], such as when performing something that is out of the ordinary for the given user, or generally perceived as important by the bank that the user should be aware of, and thus prevents the user from using his/her routine cognitive skills to complete the task.

## 2.2 Informed consent

Informed consent is the acknowledgment that the user has understood what he/she is approving. The strength of the informed consent is directly linked to how many relevant facts were presented to the user and his/her ability to understand the presented information. Pedroni and Pimple [4] describe informed consent as *'...the kind of authorisation made by a person with decision-making capacity who has a substantial understanding of the relevant information and who is free from controlling influences in making the decision.'* Another factor influencing the level of informed consent is how much control the user has when expressing his/her act-of-will.

Wu et al. [9] describe an interesting work that uses a web-wallet to help reveal the user's intention, and thereby significantly reducing phishing attacks. The web-wallet itself is, however, sensitive to spoofing itself, and does not offer good protection against Trojans. Clarke [12] outlines the principles of trust, context and consent, and proposes a framework for e-Consent, to be used on the internet. The e-Consent framework, however, does not demonstrate how to guarantee that an expressed consent comes from the user and not from malicious software, such as a Trojan.

Informed consent is established by adding relevant context to a process, which the user endorses. By forcing the user to input factual information in a context that is understandable by the user, informed consent is further strengthened. An example is where the user enters an amount when the device displays the text '*Enter amount to pay:'*. By performing this action, and entering the amount, the user expresses his/her intent.

The context stimuli or questions could be closed-ended questions, referred to as dichotomous questions, see examples in Table 2, require the users to explicitly answer "yes/no." Knowledge-based (nominal) questions is another type that requires the user to know information about something, see examples in Table 1. Nominal questions may relate either to the context or may be known only to the user, for example, a PIN. Nominal questions that relate to the context might be the monetary value of a transaction or the beneficiary in a financial transaction.

## 2.3 Risk perception

For the user to perceive risk in an action, the risk must be estimated by the bank and clearly communicated to the user. Until the risk has been understood by the user, he/she cannot estimate the risk in the action, and the risk will only be virtual, as defined by Adams and Thompson [6].

Using the computer screen to transfer risk perception to a user is not secure enough as long as malicious software may be running on the user's computer that can hide or change the details of what the user is seeing on the screen, or the user can be tricked by a phishing attack.

Communicating risk can be done in several different ways: adding context to a transaction activates a thought process in the user's brain, and by using a context that signals a certain perception, behaviour or action, the user gains higher awareness of what he/she is doing. Making the context emotional increases the user's attention, as the information he/she receives triggers emotional states, which enable the communication of risk perception. Featherman and Pavlou [10] propose a modified version of the Technology Acceptance Model (TAM), where they adopt TAM for e-services attributing to adoption/intention of e-services, and including the factors that affect the perceived risk.

## 2.4 Active participation

Adding a cognitive load in the user's process, forces the user to participate actively in the completion of the process. Active participation also goes hand in hand with risk perception and user awareness, it is a way to establish user awareness, and communicate risk perception to the user. The effort made by the user to complete the process is in relation with the risk in the transaction in combination with the risk perception received in the contextual information.

## 2.5 Trust

The basic pillars of a bank's business are trust in, and the convenience of, its products and services [7]. Banks must offer products that are trustworthy. *Trust is something that is perceived by the user* – subjectively perceived. Studies show that depending on how well something looks, the user will perform a certain action. This relates not only to web pages, but also to services in general.

## 2.6 Usability

Consumer products such as televisions are devices that a user feels comfortable to explore. When a user feels he/she cannot cause any harm to a device, it is perceived by the user to be resilient. Devices that users perceive as dangerous – where the incorrect use of the device may block the it or even cause financial loss if not operated correctly; these devices must be user-friendly, to make the user feel secure. Users are afraid of doing a traditional search and explore to understand the functions of such products [3].

Rubenstein et al. [5] show the importance of adding visual cues when a user is executing a task. Cues reduce task-switching time, where a familiar task takes significantly less time to complete than an unfamiliar one, and rule-activation time in the user's brain is related to how well the user understands the cue. A failed cue may undermine the user's process.

Degani et al. [2] discuss the normal and abnormal checklists used by pilots in the aviation industry. Pilots show a similar propensity to online banking users. Normal checklists must be short and not contain tasks that are too complex, otherwise the pilot may start overlooking them. The abnormal or emergency checklist on the other hand, contains significantly more and detailed information, but is still acceptable to the pilot, as the perceived usefulness is in relation to the perceived risk in the task.

## 2.7 Challenge questions

Challenge questions is another authentication mechanism used by a number of banks, based on shared a priori secrets. These questions and answers are used by the bank to authenticate the user, particularly for fallback scenarios, such as access to contact centres. Rabkin [8] present in their papers the usability and security aspects of personal knowledge questions. Rabkin concludes that, *'We believe that personal security questions, as currently used in fallback authentication in online banking, are surprisingly weak. [...] If current trends continue, questions of the form used today may become dangerously insecure.'* The challenge questions protocol relies on the fact that the user keeps the shared secrets secret. There is no good way for the user to protect against loss of his/her shared secrets – a phishing attack reveals those secrets.

## 2.8 Security principles

There are a number of security principles that are essential to provide a secure solution for banks: the solution should establish non-repudiation, confidentiality, integrity and consent; the solution must provide user presence. This can be established with knowledge and possession, for example, a PIN and chip card. The consent must be protected against modification by an attacker.

To provide these security principles, especially consent and user presence, we need to give this in a secure environment, outside the computer.

As the work of Johnson [14] describes: *'THE UNDERLYING HYPOTHESIS of this work is that banking fraud cannot be eliminated without a dedicated, trusted security device.'*

Johnson also proposes a USB-connected device, which has similar functionality as the solution described by Wiegold et al. [15]. This can present transaction details in the secure device, outside the reach of an attacker, where the user can approve these details. Both of these solutions only work when connected to the computer, thus adding the complexity of installation and platform dependence of software, reducing the applicability for all banks' products and service channels.

# 3. Dynamic Signatures

The Dynamic Signatures concept makes the process of authentication and authorisation visible and understandable to the user, providing a way for the user to authenticate transaction details.

The concept consists of a security device, exemplified in Figure 1, and a back-end server. Adding logic on top of the existing challenge-response scheme makes it possible for the bank to extend their business processes to include the process flows in the device. The challenge the user enters, decides the process flow in the device, when performing a normal challenge-response authentication or authorisation.

## 3.1 How it works

The concept is built on top of a traditional challenge-response scheme, where the device can generate electronic signatures on input data that the back-end server can verify. The device is capable of presenting information on the display, and accepts input from the keyboard.

**Figure 1. Example of security devices: chip card reader or token**

## 3.2 Dynamic process flow

Based on the challenge, the bank controls the process flow in the user's device. Making the process flow dynamic enables the bank to control what questions to ask the user, and when to ask them, depending on the type of transaction the user is performing. The transaction process can be seen as a series of questions, hereafter also referred to as primitive; when put together they complete the desired process flow for that user. The bank may choose what questions to ask the user, depending on the risk in the transaction or if the user needs to provide informed consent to a certain action; for example, signing a contract electronically. The questions are pre-loaded in the device. This reduces the size of the challenge, as the bank and the device shares knowledge on the pre-loaded questions, therefore the bank only needs to provide sufficient information to control which primitive questions to invoke.

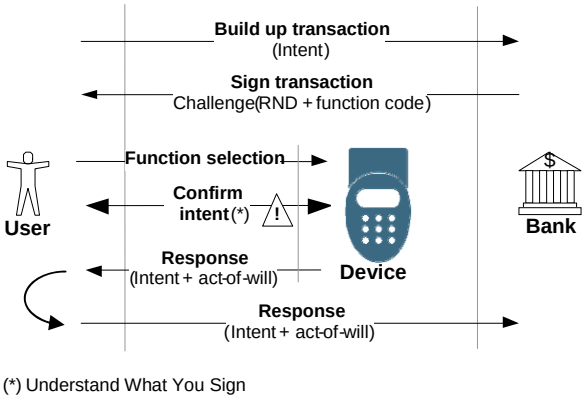


**Figure 2 Overview on security solution**

The process starts when the user has built up the transaction, which is the first step, as seen in Figure 2. The bank evaluates the received transaction request and, based on the risk and type of transaction, determines which questions to ask the user, if any. Based on this, the bank generates a challenge and requests the user to sign the challenge. Figure 3 shows an example of what the process looks like in the user's device.

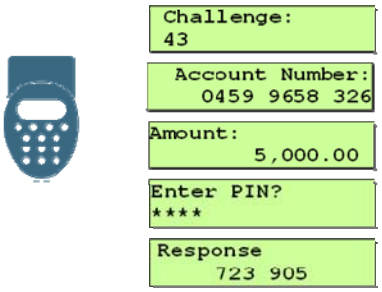


**Figure 3. Example of process flow**

The user selects the function button, as seen in Figure 4, that corresponds with the given context, for example 'Sign,' which is different from 'Login' or 'Buy.' Having separate buttons with extra text to provide context increases the user's awareness which helps prevent phishing and cross-channel attacks.


**Figure 4. Function buttons on the device**

After selecting the function, the user enters the challenge. The challenge contains three parts: a random part that establishes non-repudiation and time of transaction; a function code that selects the questions to ask the user, if any; and a check-digit that prevents the user from starting an incorrect process flow. Any of the three parts in the challenge are optional and may be excluded by the bank.

The device interprets the function code to determine which primitive questions to process. The device processes all primitives in a sequential order, where each primitive is executed sequentially, interacting with the user. Each primitive provides its own context and awareness to the user. This establish user understanding – *Transaction Authentication.* Each primitive may request input from the user for approval, or define a certain sub-process in the device. The process continues until each primitive has been successfully processed. The user is then asked to enter a PIN, '*something you know*', and the device calculates the response using the chip card, '*something you have*', and finally presents the response to the user, who then enters the response on the web page.

When the bank receives the response, the bank verifies it, and if the response is correct, this indicates a positive approval of the transaction.

## 3.3 Primitive questions

The primitive questions enable context support in the security device. Each primitive has its own functionality and context, informing the user how to complete the sub-process.

The questions for online banking are aimed at being generic, covering a broad range of transaction cases. These questions are categorised in three different groups: dichotomous questions, for example 'New beneficiary – OK?'; nominal questions, such as 'Enter amount to pay:'; and nominal questions that are only known by the user, such as 'Enter PIN:' or 'Enter your social security number:'.

For each nominal question, the customer needs to enter information. The entered information is presented together with context to the user in a familiar way during input, to provide a strong link between context and the entered information.

**Table 1. Primitive nominal questions**

| Fn# | Name | Description |
|---|---|---|
| -- | Challenge | Input of a challenge. |
| '1' | Currency | The input of currency is first. After entry of currency, the currency symbol is shown when entering amount. |
| '3' | Amount | Input of an amount. The device presents the entered amount formatted as an amount with a legend, indicating the context. |
| '4' | Beneficiary account | Input a beneficiary account. |
| '5' | Bank Identification Code | Input a Bank Identification Code. |
| '6' | Enter number of items | Input number of items. |
| '7' | Invoice ID/Reference | Input of reference number. |

**Table 2. Primitive dichotomous context messages**

| Fn# | Name | Description |
|---|---|---|
| '20' | Payment alert | 'Payment – OK?' |
| '21' | National transfers alert | 'National transfer – OK?' |
| '22' | Recurring payment alert | 'Recurring payment – OK?' |
| '23' | International transfers alert | 'International transfer – OK?' |
| '24' | Change of personal setting | 'Address change – OK?' |
| '25' | New beneficiary | 'New beneficiary – OK?' |

## 3.4 Calculation of the response

After the user has accepted all input by pressing the approval button, the primitive data is stored as a message in a data buffer according to the primitive specification. Each primitive data is uniquely identified, providing an unambiguous discrimination of each primitive that has been inputted by the user, and in which order.

The security module, for example an EMV chip card, then performs an electronic signature on the message, and the response is presented on the display.

Each primitive clearly describes its own specific functionality, adds context, and generates its own specific data. The device stores the challenge in the data buffer together with information relating to the selected function button, further describing the domain context, for example 'Login,' 'Sign transaction' or 'Buy,' to prevent cross-channel attacks.

Example of transaction:

{Challenge#1{process_flow}, Fn#1{data}, Fn#2{data}, Fn#n{data}}

To ensure integrity of the message, the encoding of primitive data is made in an unambiguous and explicit format. We have based the coding on ISO 7816-6, which is an industry standard interchange element, to specify how data elements are defined, padded and stored in the data buffer.

## 3.5 Securing user's consent

The device only generates the response after the user has correctly completed each step on the device, and approved all information. To secure the consent technically, the device generates an electronic signature over the entire message, including all information the user entered and approved. In this way, an outside attacker cannot modify what the user has approved, as the information is entered on a device. To establish that the user was present when giving his/her consent, the user is requested to provide knowledge, '*something you know*' that is a PIN, and possession, '*something you have*', that is the chip card, before the response is calculated.

Non-repudiation and time of transaction is established with information encoded in the challenge, which is included in the data buffer.

# 4. Analysis and discussion

## 4.1 Analysis

Going back and answering the questions we asked, our research shows that it is possible to make banking transactions more secure online.

By introducing context elements into the user's task process, we increase a user's awareness, where the user understands what he/she is doing. Forcing the user to participate actively, we further increase a user's awareness. By providing relevant questions that the user must answer, informed consent for a transaction can be given. When banks use these principles to pinpoint high-risk transactions, it reduces the overall risk that the user is exposed to, and thereby makes online activity more secure by involving the user. This also answers our second question.

By adding context to the function buttons on a security device, it is possible to protect against certain attacks, such as phishing, when the user is involved in online activity.

It is essential to find the correct balance between risk and usability. The banks need to keep the cognitive load for the user to a minimum for normal situations, which are considered low-risk transactions, and only request a user to confirm additional questions when there is a high-risk transaction, or a suspected fraudulent transaction. Most transactions in an online bank are considered low-risk; only 0.7% are considered as high-risk transactions.

By analysing the transaction and modelling with external information, we can predict that the risk in the transaction itself is indicated by the type of transaction, monetary value or the destination account. External information might be a user's IP address, time of day, or the behavioural profile of the current user. The bank can assess the risk in real-time and, depending on the result of the risk assessment, request the user to consent to certain information to authorise a transaction.

## 4.2 Observation of principles

The need for making online banking more secure for the user is essential, as the user is often not capable of self-protection. If a Trojan is running on a user's computer, or if the user is subjected to a Man-in-the-Middle attack, it is virtually impossible for the user to discover or prevent such attack. There is a constant battle between attackers and banks. The number of online attacks will become increasingly advanced and sophisticated, making it more and more difficult for banks to protect their users online.

Gartner carried out a survey in the US in 2005 and found that, due to security issues, 28% of online banking customers have become less active in their use of services. Out of these 28%, 77% used them less frequently; 14% stopped performing online payments; and 4% stopped using online banking. Forrester has carried out a survey in Europe with similar results.

Failure to provide secure online banking, results in the user losing trust in the service and no longer asking the bank to safeguard their money, which means banks lose business.

To make it more secure for the user online, the security solution must involve the user, to establish user awareness, where the user is able to provide his/her informed consent to the bank for a particular transaction, in a way where the consent cannot be modified by an attacker.

Below are conclusions to the principles, outlined in the earlier sections:

**User awareness:** makes it possible to establish user awareness, such as when there is a high-risk transaction that needs to be confirmed.

**Informed consent:** by requesting the user to enter information under a certain context, for example, 'Enter amount to pay:', enables the user to understand that he/she is making a payment, and by agreeing to this action, by entering the amount, the user expresses his/her consent and act-of-will back to the bank.

From a bank's perspective, paying the electricity bill or transferring a large amount of money to a new beneficiary is fundamentally different in terms of risk exposure, and for low-risk transactions, it might not be necessary to ask questions other than to establish user presence.

Establishing that the user has approved and completed the process by securing this cryptographically, prevents an outside attacker from modifying what the user has approved.

**Risk Perception:** using the computer screen to transfer risk perception to a user is not viable. A computer is not secure as long as malicious software can be running on the user's computer that can hide or change the details of what the user is seeing on the screen.

The increased participation that is the result of requesting the user to approve or input additional information in the device, strengthens the act-of-will and user's intent, which also helps provide facts that establish informed consent. User participation in the transaction communicates risk perception and strengthens the informed consent.

Communicating the risk to a user is essential. It is important to convey the risk in a particular transaction in a way that enables the user to make an informed decision in a guaranteed way.

**Active participation**: to have the user's participation in relation to the risk not only communicates risk perception to the user, it also increases usability, as most transactions are low risk, requiring low active participation. The response is the result of all questions asked, indicating that the user has participated in the transaction and provided his/her intent and act-of-will. The bank then can conclude that the user has agreed to the details.

**Usability:** a security solution must be inclusive, meaning that nearly any customer between 11 to 90 years old must be able to use the security solution. It must add sufficient cues, making the user understand what he/she is doing, which goes in hand in hand with user awareness.

**Trust: this** is achieved through a solution that is well designed, can communicate risk to the user and is able to establish informed consent. To increase the trust in the device even further, the Dynamic Signature concept uses a check-digit to prevent the user from starting an incorrect process flow in the case he/she enters a wrong challenge, which might otherwise result in loss of the user's trust in the device.

## 4.3 Wrapping up the case

The proposed Dynamic Signature concept introduces '*Transaction authentication*', the new factor in online security, as a way to establish informed consent in the authentication and authorisation process. By adding context, the authentication and authorisation process becomes visible to the user; adding it dynamically enables the bank to balance security and usability depending on the risk in the transaction. The fact that the solution is dynamic gives the bank a tool to put in the hands of the user that enables a solution to support new banking services in the future, where it is possible to mitigate risks not seen today.

The benefit of a dynamic process flow on top of an existing challenge-response scheme is that it re-uses existing well-tested

and well-defined functionality. In addition, it requires minimum effort for security practitioners to evaluate and understand the properties to adopt this new scheme, as the challenge-response scheme has already been scrutinised. Adding the context on top of a two-factor authentication solution is a cost-efficient way of establishing informed consent, to make online activity more secure.

The success criteria for the security device can be defined as: a user-friendly solution, which anyone is able to use without the need of search and explore; having logical functionality that enables the user to understand the process flow of the device and enables the user to understand the reason of usage; a device that does not have cryptic texts that are difficult to understand; a device that is programmed to "I-follow-you" principles; a device that does not contain any transitory messages that disappear after a short period of time, and that has context support. If cumbersome, people will stop using a device, therefore, it should be portable so that it can be used by anyone, anywhere and anytime.

## 5. Conclusions

Making the process clear to the user, by adding descriptive text to function buttons on the security device, we increase the user's awareness, whereby the user understands what he/she is doing, making online activities more secure.

Introducing context elements into the user's task process, we increase a user's awareness, where the user understands what he/she is doing. Forcing the user to participate actively, we further increase a user's awareness. By providing relevant questions that the user must answer, the user is able to give his/her informed consent to a transaction. When banks use these principles to pinpoint high-risk transactions, we reduce the overall risk that the user is exposed to, and thereby make online activity more secure by involving the user.

We have proposed a concept, Dynamic Signatures, that introduces a new factor to online security – '*Transaction authentication*'. The solution provides security while minimising user involvement, by balancing security and usability. By making the user involvement dynamic, the solution can adapt to new risks not seen today. It also enables quick adoption to new banking services. By invoking context into the user's task process, having the user participate actively, we further increase the user's awareness. By providing relevant questions, that the user is asked to answer, the user is then able to give his/her informed consent to a transaction. When banks use these principles to pinpoint high-risk transactions, we reduce the overall risk that the user is exposed to, and thereby make online activity more secure by involving the user.

## 6. Acknowledgments

Thanks go to Simone Fischer-Hübner, Anna Börjesson-Sandberg, Gustaf Björklund, Björn Eriksson, John Ahlberg, and Håkan Nordfjell for providing helpful comments and reviewing this paper.

## 7. References

[1] Tygar, J. D.; Whitten, Alma, WWW electronic commerce and Java Trojan horses, Proceedings of the Second USENIX Workshop on Electronic Commerce}, (1996), pp. 243-250

[2] Degani, Asaf and Wiener, Earl L., Human Factors of Flight-Deck Checklists: The Normal Checklist. Moffett Field, California : NASA, 1990.

[3] Norman, Donald A., Emotional Design: Why We Love (or Hate) Everyday Things., Basic Books, 2003.

[4] Pedroni, Ph.D. Julia A. and Pimple, Ph.D. Kenneth D., A Brief Introduction to Informed Consent in Research with Human Subjects, Indiana University, June 2001. Scientists and Subjects: A Web-Based Seminar on the Ethics of Research with Human Subjects. pp. 13.

[5] Rubenstein, Joshua S.; Meyer, David E. and Evans, Jeffrey E., Executive control of Cognitive Processes in Task Switching: Human Perception and Performance., 4, 2001, Journal of Experimental Pshycology, Vol. 27, pp. 763-797.

[6] Adams, John; Thompson, Michael, Taking account of societal concerns about risk Framing the problem, Health and Safety Executive, 2002, [Online] Decmeber 2008, www.hse.gov.uk/research/rrpdf/rr035.pdf

[7] Hertzum, Morten; Juul, Niels Christian; Jørgensen, Niels; Nørgaard, Mie, Usable Security and E-Banking: Ease of Use vis-à-vis Security, OZCHI 2004 Conference Proceedings, Roskilde University, Denmark, 2004

[8] Rabkin, Ariel, Personal knowledge questions for fallback authentication: Security questions in the era of Facebook, Symposium on Usable Privacy and Security (SOUPS), 2008, pp. 13-23, ACM press

[9] Wu, Min; Miller, Robert C.; Little, Greg, Web wallet: Preventing phishing attacks by revealing user intentions, In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2006, pp. 102-113, ACM press

[10] Featherman, Mauricio; Pavlou, Paul A., Predicting E-Services Adoption: A Perceived Risk Facets Perspective, (2003), International Journal of Human-Computer Studies, 59, 4, pp.451—474

[11] Drimer, Saar; Murdoch, Steven J. and Ross Anderson, Optimised to Fail: Card Readers for Online Banking, Financial Cryptography and Data Security '09, [Online] February 2009, http://fc09.ifca.ai/papers/58_Optimized_to_fail.pdf

[12] Clarke, Roger; eConsent: A Critical Element of Trust in eBusiness Abstract (2002) 15th Bled Electronic Commerce Conference, eReality: Constructing the eEconomy

[13] Dey, Anind K.; Understanding and using context, Personal and Ubiquitous Computing, (2001), Vol(5), pp.4—7

[14] Johnson Matthew, A new approach to Internet banking, 2008, University of Cambridge, [Online] February 2009, www.cl.cam.ac.uk/techreports/UCAM-CL-TR-731.pdf

[15] Weigold, Thomas; Kramp, Thorsten; Hermann, Reto; Höring Frank; Buhler, Peter; Baentsch, Michael; The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks, IBM Zurich Research Laboratory, 2008, [Online] February 2009, www.zurich.ibm.com/pdf/csc/ZTIC-Trust-2008-final.pdf