Usability Heuristics for Web Banking

Natali Fierro[1] and Claudia Zapata[2](✉)

[1] Maestría en Informática, Pontificia Universidad Católica del Perú, Lima, Peru
nfierrod@pucp.pe

[2] Doctorado en Ingeniería, Pontificia Universidad Católica del Perú, Lima, Peru
zapata.cmp@pucp.pe

Abstract. The rapid development of technology has changed the way in which humans and computers interact. This revolution is no stranger to the banking sector, there is a tendency to migrate the services offered by financial institutions face channels to remote channels. This research will focus on the study of the applications of web banking, and through the analysis of the problems it faces, it will seek to establish design guidelines in the form of evaluation methods that allow us to measure the degree of usability of a site, thus contributing to the increase in the degree of user satisfaction by improving the usability of these applications. To achieve this goal, a set of proposed usability heuristics; these also consider issues relating to safety. The proposed heuristic was evaluated in order to compare their effectiveness in contrast to existing heuristics.

Keywords: Usability · Heuristics · Web banking

1 Introduction

The emergence of web banking has been accompanied by a new type of menace for end users: cyber fraud [2, 9, 10]. According to the FFA (Financial Fraud Action), the losses caused by cyber fraud in the UK had an increase of 48 % in 2014 [20]. These events have compromised the user confidence in the web banking, causing the consumers show refusal to conducting their financial operations via online transactions, a phenomenon that is particularly evident in developing countries [5, 6].

In an effort to counter the mistrust associated with the use of web banking, the banks have focused their efforts on developing solutions that deliver high levels of security. However, this emphasis on security has resulted in an increase in the perceived complexity compromising usability [3].

Taking into consideration that several authors argue that characteristics such as quality, perceived safety and usability significantly influence user satisfaction and consequently on the intended use of a site [15, 18], then to promote the adoption of web banking solution is necessary that the increase in the perceived safety goes together with improved usability [1].

Unfortunately most of the time the relationship between security and usability is inversely proportional [9]. Moreover, there are few studies focusing on the importance of the interrelationship of these factors in the field of web banking, and existing work has focused solely on the study of the choice of authentication solutions [1, 3, 9], paying little attention to the usability of the interface as such.

A. Marcus (Ed.): DUXU 2016, Part I, LNCS 9746, pp. 412–423, 2016.
DOI: 10.1007/978-3-319-40409-7_39

It exposed a web banking must be designed and evaluated considering its ease of use and security levels, for which it is required: design guidelines and evaluation methods usability.

2 Heuristic Evaluation and Web Banking

A systematic review of the literature related to usability evaluation was performed on web services, considered as relevant in order to study the work related to the heuristic evaluation usability in e-commerce, transactional services and e-government, and others.

Relevant studies were selected through electronic search in four recognized data bases: Scopus, IEEE Xplore, Science Direct and ACM Digital Library. The keywords used in the search strategy for primary studies were: usability, e-commerce, transactional, e-banking, online, checklist, guidelines, heuristic. The results obtained were filtered based on a review of the title and the abstract; the selected studies are presented below.

2.1 Usability and Transactional Web Services

Paz et al. [14] expose the need for appropriate usability heuristics for evaluating emerging new software products. This premise is verified for transactional web services through a case study. Their work proposes the use of a set of fifteen new usability heuristics for evaluating specific transactional web services.

Meanwhile Garrido et al. [4] studied the problems experienced by users when using electronic processing services offered by their governments. A diagnosis of the state of services electronic procedure is carried out by conducting usability heuristic evaluations sixty transactional services offered by institutional pages of the Chilean government. Their results report usability problems mainly in the following points: (1) user control and freedom, (2) perceived sense of uncertainty (3) absence of user guides. They conclude that usability is an important factor in explaining the slow growth and distrust expressed by users when using a service electronic process variable.

In turn Hughes et al. [7] present a heuristic evaluation tool to assess the usability of financial analysis tools provided in institutional pages from five different countries around the globe. His proposal consists of fourteen heuristics based on the work of Wenham et al. [17].

2.2 Usability and Security

Gonzalez et al. [5] used the approach GQM (Goal Question Metric) and heuristics Johnston et al. [8] to propose a set of metrics to measure the usability and security in e-commerce applications. In addition, they propose a methodology for the design of safe and usable websites [6].

For Nurse et al. [13], usability is one of the most important aspects to consider when designing secure systems because a non-usable system results in improper application of the mechanisms and security policies. With the aim to contribute to obtaining usable and secure applications, consolidate a number of existing general "guidelines" applicable to design usable systems with emphasis on safety.

2.3 Usability and Web Banking

One of the first works on usability in web banking is reported by Wenham and Zaphiris [17], which conducted a review of existing usability evaluation methods and select the most appropriate for assessing implementation of electronic banking. The selected methods are then applied to two case studies and the effectiveness of each method is analyzed. Based on the results propose a set of twelve heuristics to use in evaluating the usability of electronic banking.

Mujinga et al. [11] emphasizes in the vulnerabilities that are exposed web banking users and the necessity to consider usability when designing a secure system. Based on the Nielsen heuristics [12] proposes a heuristic model, consisting of a set of sixteen heuristics, in order to facilitate the design and development of a safe and usable web banking.

3 Methodology

The set of heuristics was obtained using the methodology proposed by Rusu et al. [16], it can be described through six stages (Fig. 1).

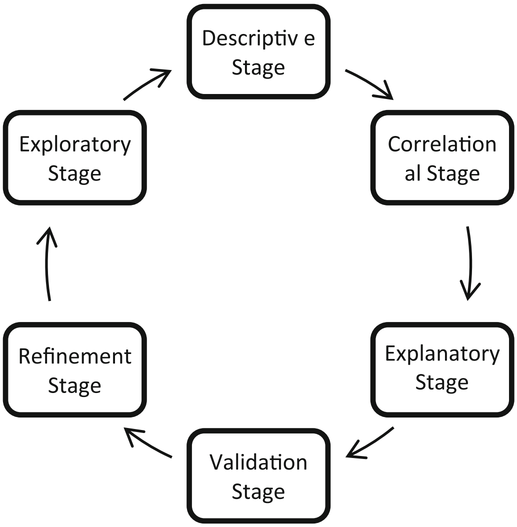


Fig. 1. Methodology

- Exploratory stage: a review of literature related to Internet banking, transactional web services, and security was made.
- Descriptive stage: the most important features of the previously collected information are highlighted, emphasizing aspects related to usability and safety.
- Correlation stage: the main features are identified that a proposal for usability heuristics for web banking should consider, based on Nielsen heuristics.
- Explanatory stage: the set of heuristics proposals formally specified by using a standard template.
- Validation stage: heuristic proposals are validated by performing a heuristic evaluation usability on a previously selected case study, comparing their performance with Nielsen heuristics. In addition, surveys were performed to obtain the appreciations of experts on the proposed heuristics for web banking.
- Refinement stage: were modified some of the heuristics proposals based on feedback obtained from the previous stage.

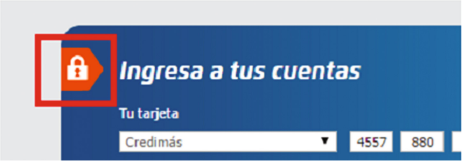
4 The Proposed Heuristics

Following the methodology described in the previous section has been obtained the set of usability heuristics presented below:

4.1 BIH1 Confidence

Users need to feel a sense of confidence in using the system. Security measures must be visible, user friendly and accessible; you must explain to users how to use the site and the safest way to send alerts when necessary.

Example: Fig. 2 shows a section of the home page of the web banking of Banco de Crédito del Perú (https://www.viabcp.com/wps/portal/viabcpp/personas). The use of the symbol "lock" associated with section "Join your Accounts" transmits the feeling of entering a secure site.



Ingresa a tus cuentas

Tu tarjeta

Credimás ▼ 4557 880

Fig. 2. Example of BIH1 Confidence

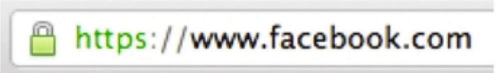
4.2 BIH2 Navigability

Navigation of the site must be logically structured and should allow the user to easily move from one place to another. Information should be organized in such a way that the user can easily interact with the system when making a transaction.

4.3 BIH3 Visibility of System Status

Users should be informed of the internal state of the system and state security mechanisms.

Example: Fig. 3 shows the use of iconography to indicate that a security feature of the system is active.



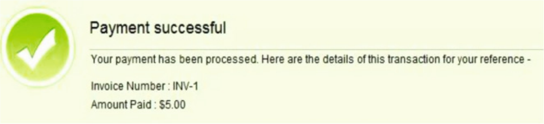
https://www.facebook.com

Fig. 3. Example of BIH3 Visibility of System Status

4.4 BIH4 Transaction Status

The system must inform users within a reasonable time, about the success or failure of the transaction.

Example: Fig. 4 shows the use of a notice accompanied by iconography to indicate the status of the execution of a payment transaction.



Payment successful

Your payment has been processed. Here are the details of this transaction for your reference -

Invoice Number : INV-1
Amount Paid : $5.00

Fig. 4. Example of BIH4 Transaction Status

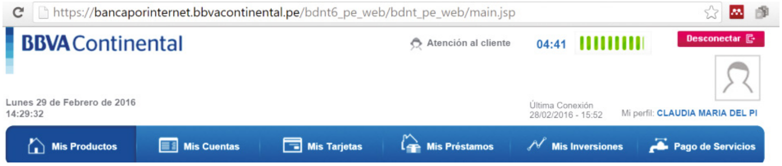
4.5 BIH5 Familiarity

The system should employ elements, phrases and concepts familiar to the user. They must be used metaphors and dialogues of the real world. The concepts related to security should also be presented in a manner familiar to the user.

4.6 BIH6 Customizing

Users should be free to customize the system interface, including security features, according to their preferences.

Example: Fig. 5 shows the use of customizing of web banking of BBVA Continental (https://www.bbvacontinental.pe). At the top it shows that you can upload a photo.



https://bancaporinternet.bbvacontinental.pe/bdnt6_pe_web/bdnt_pe_web/main.jsp

Lunes 29 de Febrero de 2016
14:29:32

Última Conexión
28/02/2016 - 15:52

Mi perfil: CLAUDIA MARIA DEL PI

Fig. 5. Example of BIH6 Customizing

4.7 BIH7 Freedom and User Control

The system must provide support for undo and redo actions. Users could choose a system function by mistake, and they would need a clearly marked exit to leave the undesired state without having to perform many steps.

When possible, it should be allowed users to revoke decisions already taken, including decisions on security measures.

4.8 BIH8 Consistency and Standards

Users should not hesitate if situations, words or different actions mean the same thing. It is very important to maintain a similar design throughout the interface. The website should be consistent not only internally, but consistent with similar sites.

4.9 BIH9 Clarity

The interface should communicate in a simple and concise manner using the language of the user, must transmit the available security features clearly and using appropriate language.

4.10 BIH10 Minimize User Memory Load

The user should not be forced to remember information from a previous state.

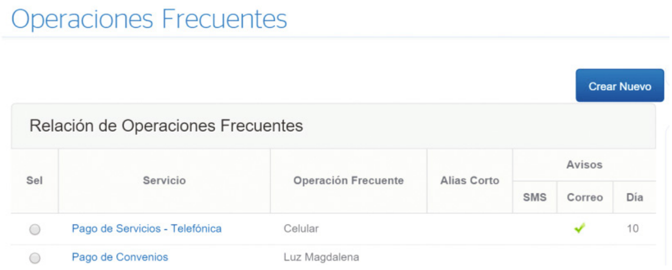
System instructions should be easy to remember through highly intuitive interfaces. It could include easy configuration of system security, reduce the number of security decisions that users should take.

4.11 BIH11 Flexibility and Efficiency in Use

The system must provide enough information for novice users, without providing too much information for experienced users.

While novice users may need assistance step by step, expert users should be able to quickly access functionality required by shortcuts.

Example: Fig. 6 shows the correct use of the flexibility and efficiency in use by frequent operations functionality.



Operaciones Frecuentes

Relación de Operaciones Frecuentes

Sel	Servicio	Operación Frecuente	Alias Corto	Avisos		
				SMS	Correo	Día
○	Pago de Servicios - Telefónica	Celular			✓	10
○	Pago de Convenios	Luz Magdalena				

Fig. 6. Example BIH11 Flexibility and Efficiency in Use

4.12 BIH12 Aesthetic and Minimalist Design

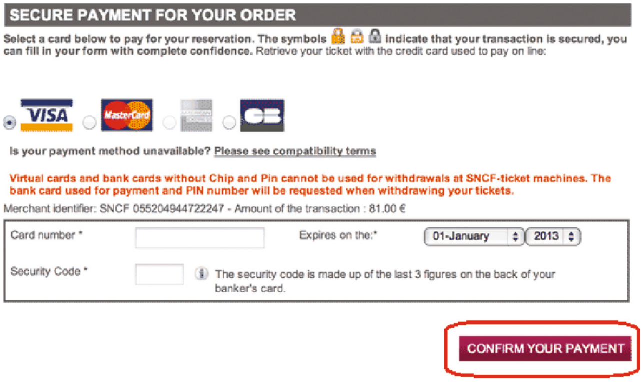
Dialogues should not contain information irrelevant or that is rarely used. Every extra unit of information competes with relevant information units and decreases their relative visibility. The interface should contain only relevant for the system or for information security mechanisms. It should not overwhelm the user with information, should reduce the number of settings, passwords to remember.

4.13 BIH13 Error Prevention

Even better than good error handling is a careful design which prevents the occurrence of problems. It is recommended to eliminate error-susceptible conditions or a verification of the same, asking the user for confirmation before performing an action.

Users should know the consequences of any action related to safety, irreversible actions must be clearly marked.

Example: Fig. 7 shows the use of a confirmation button, this mechanism serves to prevent the execution of a payment transaction unwanted.



SECURE PAYMENT FOR YOUR ORDER

Select a card below to pay for your reservation. The symbols indicate that your transaction is secured, you can fill in your form with complete confidence. Retrieve your ticket with the credit card used to pay on line:

Is your payment method unavailable? Please see compatibility terms

Virtual cards and bank cards without Chip and Pin cannot be used for withdrawals at SNCF-ticket machines. The bank card used for payment and PIN number will be requested when withdrawing your tickets.

Merchant identifier: SNCF 055204944722247 - Amount of the transaction : 81.00 €

Card number * Expires on the:* 01-January 2013

Security Code * The security code is made up of the last 3 figures on the back of your banker's card.

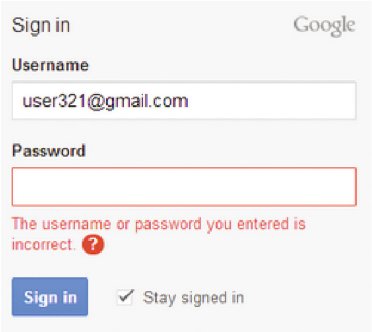
Fig. 7. Example BIH13 Error Prevention

4.14 BIH14 Helps the User to Recognize, Diagnose and Recover from Mistakes

Error messages should be expressed in clearly language indicating precisely the problem and suggest a solution. If an error occurs should be handled properly.

It should provide users detailed error messages, do not use codes and then allow recovery through simple mechanisms. Care should be taken not to compromise the security of the site to return information about the error occurred.

Example: Fig. 8 shows the correct use of aid the user to recognize, diagnose and recover from errors. It appreciated the use of an informative message about the error produced, it is noteworthy that security is not compromised because no details if the error is in the user or password.



Username
user321@gmail.com

Password

The username or password you entered is incorrect. ?

Fig. 8. Example of BIH14 Helps the user to recognize, diagnose and recover from mistakes

4.15 BIH15 Help and Documentation

Although the ideal is that a system can be used without documentation, it is necessary to provide help and documentation. This information should be easy to search, focused on the user's task, list concrete to do and not be too long steps.

Users should be able to easily locate and view online help and documentation system should include documentation of security features. It should also provide recommendations when the user is unsure of a decision and its implications.

5 Validating the Proposal

To validate the usability heuristics, the methodology proposed by Rusu et al. [16], which is to employ two groups working on the same case study on equal terms used.

Usability problems that are identified by each of the groups to be compared using the following criteria:

- P1 - Problems identified by both groups of evaluators
- P2 - Problems identified only by the group using the heuristic proposals
- P3 - Problems identified only by the group using traditional heuristics (Nielsen).

The new usability heuristics work well when:

- P2 includes the highest percentage of usability problems or
- P1 + P2 include the highest percentage of usability problems

However, if the set P3 includes the highest percentage of usability problems, you must discard the following assumptions:

- H1 - The new heuristics failed to identify many usability problems because they are not properly specified.
- H2 - The evaluators who used the new heuristics ignored subjectively problems.

To validate or reject each of these assumptions will be necessary to make further experiments.

5.1 Case Study

The case study selected to perform the validation of the new set of heuristics was the web banking BBVA Continental (https://www.bbvacontinental.pe/personas/).

The choice of this application as an object of study is justified the participation of BBVA Continental in Peru's banking system, standing at year-end 2014s in loans and deposits and third in economic terms.

Each evaluator is asked to enter the web banking BBVA Continental and perform the following tasks:

- Payment of studies at the Catholic University of Peru
- Consultation savings account balance
- Transfer of funds between accounts
- Querying account credit card

5.2 Evaluation Based on Heuristic Nielsen

Then all the problems associated with each heuristics are presented. It may be observed that the highest percentage of problems (36 %) was associated with heuristics number two "Match between system and the real world" (Table 1).

Table 1. Broken heuristics - Nielsen

ID	Heuristics	Number of problems
NIH1	Visibility of system status	0
NIH2	Coincidence between the system and the real world	8
NIH3	User control and freedom	3
NH4	Consistency and standards	1
NH5	Error prevention	2
NH6	Recognition	2
NH7	Flexibility and efficiency of use	1
NH8	Aesthetic and minimalist design	3
NH9	Helps users recognize, diagnose and recover from mistakes	2
NH10	Help and documentation	0

5.3 Evaluation Based on the New Proposal

Below is all the problems associated with each heuristics are presented. It can be observed that none of them was heuristics associated a percentage significantly higher compared to other problems. Should be noted, the heuristics did not have a counterpart in Nielsen (“BIH1-Confidence”, “BIH6- Customizing”), together obtained 12 % (Table 2).

Table 2. Broken heuristics - Proposal

ID	Heuristics	Number of problems
BIH1	Confidence	2
BIH2	Navigability	3
BIH3	Visibility of system status	0
BIH4	Transaction status	0
BIH5	Familiarity	1
BIH6	Customizing	1
BIH7	Freedom and user control	4
BIH8	Consistency and standards	1
BIH9	Clarity	2
BIH10	Minimize user memory load	2
BIH11	Flexibility and efficiency in use	4
BIH12	Aesthetic and minimalist design	2
BIH13	Error prevention	2
BIH14	Helps the user to recognize, diagnose and recover from mistakes	1
BIH15	Help and Documentation	2

5.4 Comparative Analysis

In this section the results of heuristic evaluations by the two groups are listed.

- P1 - Problems identified by both groups of evaluators: 20 %
- P2 - Problems identified only by the group using the heuristic proposed: 46 %
- P3 - Problems identified only by the group using traditional heuristics (Nielsen): 34 %

To compare the detected problems using both proposals, Nielsen heuristics are mapped with the proposals as shown in Fig. 9.

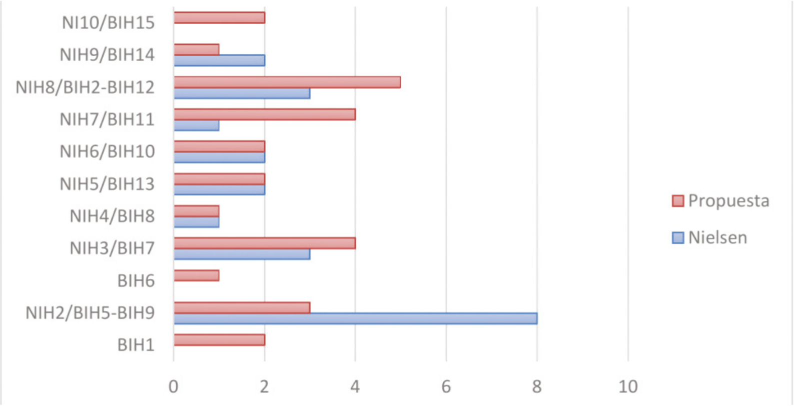


Fig. 9. Problems detected

6 Conclusions and Future Work

The methods, techniques and tools existing for evaluating usability of software applications focus on the characteristics of generic interfaces. However, the web banking has intrinsic to their domain particularities. Therefore, having a specific assessment tool to analyze the usability of these applications is necessary.

This research can develop a theoretical proposal that can integrate security features in usability evaluation of web banking. However, it is important to note that there are certain factors that could influence the data presented in this research, such as the availability of evaluators, the degree of familiarity with the application assessed, among others.

Through the experiments conducted it was determined that the Nielsen heuristics have some limitations when applied to the domain under study, it was observed that most problems identified corresponded to the aesthetic design and the use of metaphors. In contrast, the problems encountered by the proposal concentrated around flexibility and user control. Additionally, it should be noted that the proposal allowed the detection of problems associated with security features, which were not detected by the control group.

Consequently, replication of the experiment in other implementations banking web is necessary. Including implementations made not only by banks but also by financial institutions oriented small businesses, which will allow better analysis of the performance of the proposed heuristics.

References

1. Althobaiti, M.M., Mayhew, P.: Security and usability of authenticating process of online banking: User experience study. In: 2014 International Carnahan Conference on Security Technology (ICCST), pp. 1–6 (2014)

2. Costante, E., et al.: On-line trust perception: What really matters. In: 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), pp. 52–59 (2011)
3. French, A.M.: A case study on e-banking security-When security becomes too sophisticated for the user to access their information. J. Internet Bank. Commer. **17**(2), 1–14 (2012)
4. Garrido, M. et al.: Usability problems and lines of solutions: an expert evaluation of Chilean online services. In: Proceedings of the 2013 Chilean Conference on Human - Computer Interaction, pp. 76–81. ACM, New York (2013)
5. Gonzalez, R.M. et al.: A measurement model for secure and usable e-commerce websites. In: Canadian Conference on Electrical and Computer Engineering, 2009, CCECE 2009, pp. 77–82 (2009)
6. Gonzalez, R.M. et al.: A pattern methodology to specify usable security in websites. In: 20th International Workshop on Database and Expert Systems Application, 2009, DEXA 2009, pp. 155–159 (2009)
7. Hughes, J., et al.: A heuristic evaluation instrument for e–government online software. Electron. Gov. Int. J. **10**(1), 1–18 (2013)
8. Johnston, J., et al.: Security and human computer interfaces. Comput. Secur. **22**(8), 675–684 (2003)
9. Mockel, C.: Usability and security in EU E-banking systems - towards an integrated evaluation framework. In: 2011 IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT), pp. 230–233 (2011)
10. Montazer, G.A., ArabYarmohammadi, S.: Identifying the critical indicators for phishing detection in Iranian e-banking system. In: 2013 5th Conference on Information and Knowledge Technology (IKT), pp. 107–112 (2013)
11. Mujinga, M., et al.: Towards a heuristic model for usable and secure online banking. In: 24th Australasian Conference on Information Systems (ACIS), pp. 1–12. RMIT University (2013)
12. Nielsen, J.: Usability Engineering. Morgan Kaufmann, California (1993)
13. Nurse, J.R.C., et al.: Guidelines for usable cybersecurity: Past and present. In: 2011 Third International Workshop on Cyberspace Safety and Security (CSS), pp. 21–26 (2011)
14. Paz, F., et al.: Usability heuristics for transactional web sites. In: 2014 11th International Conference on Information Technology: New Generations (ITNG), pp. 627–628 (2014)
15. Riffai, M.M.M.A., et al.: Big TAM in Oman: Exploring the promise of on-line banking, its adoption by customers and the challenges of banking in Oman. Int. J. Inf. Manag. **32**(3), 239–250 (2012)
16. Rusu, C., et al.: A methodology to establish usability heuristics. In: ACHI 2011, The Fourth International Conference on Advances in Computer-Human Interactions, pp. 59–62 (2011)
17. Wenham, D., Zaphiris, P.: User interface evaluation methods for internet banking web sites: a review, evaluation and case study. In: Human-Computer Interaction: Theory and Practice, pp. 721–725 (2003)
18. Yoon, H.S., Steege, L.M.B.: Development of a quantitative model of the impact of customers' personality and perceptions on Internet banking use. Comput. Hum. Behav. **29** (3), 1133–1141 (2013)
19. Zhang, H.: The study on evaluation of e-banking web sites from the viewpoint of customers. In: 2010 International Conference on Computer Design and Applications (ICCDA), pp. V2-263–V2-266 (2010)
20. Scams and computer viruses contribute to fraud increases - calls for national awareness campaign. http://www.theukcardsassociation.org.uk/news/EOYFraudFigs2014.asp