Originally published in GI-Edition Lecture Notes in Informatics vol. 232:
"INFORMATIK 2014 Big Data – Komplexität meistern", 2014, pp. 2093 - 2104

"A Bank Would Never Write That!" A Qualitative Study on E-Mail Trust Decisions

Thomas Pfeiffer, Michaela Kauer and Julia Röth
Institute of Ergonomics
Technische Universität Darmstadt, Otto-Berndt-Straße 2
64287, Darmstadt

t.pfeiffer@iad.tu-darmstadt.de; kauer@iad.tu-darmstadt.de; julia.roeth@gmx.de

Abstract: In order to communicate the risk of fraudulent e-mails to users properly, it is important to know which aspects they focus on when evaluating the trustworthiness of an e-mail. To that end, a study was conducted to test predictions derived from a decision model by asking participants how they would react to each of eight e-mails and why. The study confirms results from previous research showing that content as well as visual and linguistic aspects, but also technical aspects such as sender address and link URL are considered by recipients. It also adds new findings like the fact that through experience and education, users form rules such as "A bank will never ask you for account details via e-mail" or the fact that attachments in HTML format or implausible sending times raise suspicions in users. These findings can be used to inform the design of anti-fraud education and user interfaces of e-mail clients.

1 Introduction

One of the most prominent risks of e-mail communication is the exposure to malicious e-mails which aim to trick recipients into giving away sensitive information (phishing), transferring money (e.g. the so-called "Nigerian" or "419" scam [SW11]) or opening malicious attachments. In order to support users in protecting themselves from these risks, they have to be communicated to them either through preventive education or through the user interface of (web, desktop or mobile) e-mail clients. To optimally target these communication efforts, it is important to first learn which aspects users focus on when deciding how to react to an e-mail, in order to identify in which aspects their behavior has to be improved. This paper covers a study which aims to both confirm results from previous research which on this topic and to uncover aspects relevant to users which have not been documented yet.

The paper is structured as follows: Section 2 describes the model we created and which this study is based on, and the research questions derived from it. Section 3 documents the methods used in the study, the results of which are detailed in section 4 and discussed in section 5. Section 6 concludes the paper and offers an outlook on the application of the results and on further research.

2 Background and Research Questions

The study presented in this paper is based on a model to predict recipients' reactions to calls to action contained in online messages, which was presented by Pfeiffer, Theuerling and Kauer [PTK13]. That model is based on results from previous research on user reactions to e-mails and websites from both the social engineering and e-commerce fields (see aforementioned paper for details, as they do not fit into this paper's space limit). It contains several sets of variables that influence recipients' reactions: attributes of the message, attributes of the purported sender, attributes of context, knowledge/experience of recipient, demographic attributes of recipient, and personality traits of the recipient. Using interviews, the study presented in this paper focuses on the attributes of the message and purported sender as well as contextual factors which influence recipients' reactions.

The attributes of the message predicted to influence reactions are URLs of links (including whether they start with https), the subject line, design aspects such as company/brand logos and colors, trust seals, language (including spelling and grammar errors), personalization (such as inclusion of the recipient's name or account number), the presence of a footer with company and legal information, the overall narrative strength of the e-mail's content, the quality of the (additional) information and content provided in the e-mail, a perceived persuasion attempt, and perceived privacy and security protection communicated through the e-mail. The aspects of the e-mail's (purported) sender which are predicted to influence recipients' reactions are the name and address in the "from" field, familiarity with (receiving e-mails from) the sender, as well as the (purported) sender's reputation. Contextual aspects are the contextual plausibility of the e-mail (for example whether an order the message is referring to was actually placed by the recipient). Another contextual aspect, recipient's computer's perceived vulnerability to attacks, is not expected to be of relevance to participants of this study because it presents a fictitious scenario where participants cannot assess the computer's vulnerability.

3 Methods

The study took place in 2013 in a lab at the Technische Universität Darmstadt and consisted of a questionnaire before and interviews after participants were shown examples of authentic and fraudulent e-mails. It was one part of a larger setup which also included eye tracking and the presentation of e-commerce websites (all of which were authentic). Due to space limitations, this paper only reports the results from the interviews. After an introduction, participants filled in an online questionnaire. It contains questions on socio-demographic information (age, gender, educational level and monthly household income) as well as experience with and usage of the Internet and electronic devices, and the familiarity with software used in the study.

After completing the questionnaire, participants were shown eight different e-mails in Portable Document Format in randomized order, each of them twice. PDFs had to be used due to restrictions in the eye tracking software. The set of e-mails consist of four

authentic commercial e-mails and four real-world phishing examples. If they contain links whose URL is not directly visible, it is included at the bottom of the PDF since it is not possible to use mouse-over to see the URL in the PDF. Except for the fraudulent e-mail purportedly from Facebook (written in English), the e-mails are written in German. In the following descriptions, text is translated.

Table 1 and 2 detail the characteristics of the e-mails with regard to the features mentioned in section 2, tables 3 and 4 do the same for the fraudulent ones. URLs are shortened to the domain names (or other domain names contained elsewhere in the URL).

Purp. sender	**comdirect bank**	**Amazon Marketplace**
"From" address	comdirect.postbox@noreply.comdirect.de	Solution 21 - Amazon Marketplace <chp00fxqpq4225@ marketplace.amazon.de>
Subject	PostBox: You have received a new financial report	Receipt-201216235
Link URLs	www.comdirect.de	www.amazon.de/..., www.adobe.com/...
Design/layout	Plain text	Plain text
Language	Professional, no errors	Professional, no errors
Form of address	Impersonal	Impersonal
Signature	comdirect bank AG	Kind regards
Other personaliz.	Last 3 digits of account-no.	None
Footer	Company info with link to website	None
Story	Information about available financial report	Information about invoice incl. number and date (no need for payment implied)
Call to action	Go to personal area on website (no link)	None (implicit: read invoice)
Additional info	Best bank award	Info on Adobe Reader required to read PDF incl. download link
Priv./Sec. info	Info can be unsubscribed from	Info on secure online purchasing, security and anonymity features of Amazon Marketplace e-mail system
Attachment	None	Invoice-201216235-16307.pdf

Table 1: Features of Authentic E-mails

When seeing the e-mails for the first time, participants were instructed to look at them carefully and form an opinion about them (while there eye movement was being tracked). After that, the same e-mail was shown a second time and the experimenter asked them how they would have reacted to the e-mail and for which reasons, as well as which features of it they noticed and whether they have influenced their opinion. The e-mails were shown twice in order to separate the eye-tracking from the interview part but still allow participants to point out the aspects they looked at in the e-mails. Their answers were

Purp. sender	**Zalando**	**Facebook**
"From" address	Zalando Team <team@info.zalando.de>	Facebook <update+kjdmwwjmvi5m@facebookmail.com>
Subject	Your new password at Zalando	Juli, you have unread notifications
Link URLs	www.zalando.de/...	www.facebook.com/login.php/..., www.facebook.com/o.php/...
Design/layout	Logo, fonts, colors, two trust seals	Facebook logo and other icons
Language	Professional, no errors	Informal, no errors
Form of address	Personal	Personal
Signature	Kind regards, your Zalando team	None
Other personaliz.	None	E-mail addr. contained in login link
Footer	Detailed comp. and contact info	Postal address
Story	Link to reset password at user's request	Info about unread notifications
Call to action	Click link, enter new password	Click link to read messages
Additional info	Link only valid for 24h, advertisements	None
Priv./Sec. info	None	Info for unsubscribing from news service
Attachment	None	None

Table 2: Features of Authentic E-mails Part 2

noted down in shortened form by the experimenter. Afterwards, participants were shown the e-commerce websites and filled out a second questionnaire. These parts, however, are not relevant to the results presented in this paper, since they happened after these results were gathered.

Participants were recruited by Julia Roeth from her private and academic social networks. There was no compensation for participating in the study, participation was completely voluntary.

4 Results

4.1 Sample

The study had a total of 34 participants, eight of which were female. The age ranged from 20 to 66, with a median of 25 years. One participant had an intermediate school-leaving certificate, two had a qualification for entrance to universities of applied science. Fifteen

Purp. sender	**Facebook**	**Bank**
"From" address	Facebook administration <heedonghong@ftp3.scmedia.com.hk>	Bob Daslamm <bobdaslamm@gmx.de>
Subject	'You have 1 personal notification from Facebook Administration	Account blocked, assistance required
Link URLs	http://cp990.perso.sfr.fr/...	http://wwwbanksq.biz/?meine.deutsche-bank.de/...
Design/layout	Facebook logo and other icons	Plain
Language	Informal, no errors	Simple, no errors, missing spaces
Form of address	None	Impersonal
Signature	None	MariaWolf
Other personaliz.	Part of e-mail address in link	None
Footer	Postal address	None
Story	Info: Message from Facebook administr. waiting for response	Bank account blocked due to suspicious actions
Call to action	Click link to read message	Click link to activate update and restore access
Priv./Sec. info	None	None
Attachment	None	None

Table 3: Features of Fraudulent E-mails

participants had a general university entrance qualification, 16 had a degree from a general university or a university of applied sciences.

All participants used the internet daily. 24 participants had been using the internet for more than 10 years, nine for 7 to 10 years and one participant for 3 to 7 years.

4.2 Methods of Analysis

The reasons given for the participants' reactions to each e-mail (from the experimenter's notes) were categorized and for each participant and each e-mail it was recorded whether a category was not mentioned at all, mentioned as supporting the decision or as contradicting the decision. Then the total number of mentions of each category and the number of participants which mentioned a category at least once were counted.

4.3 Predicted Features

At first, the aspects predicted by the model to influence the decision (see section 2) are analyzed. Table 5 illustrates the number of mentions of these features as well as how many

Purp. sender	**PayPal**	**Visa/Mastercard**
"From" address	PayPal.de <Service@paypal-europa.biz>	Visa und Mastercard <service@visa.de>
Subject	PayPal - account	Important message from Visa / Mastercard
Link URLs	http://support.paypal-service-europa.biz/ .../verify_account	None
Design/layout	PayPal logo + colors, icons (all look cut out)	Plain
Language	Professional, only one capit. error	Low linguistic quality, errors, encoding problem
Form of address	Impersonal	Impersonal
Signature	None	Regards
Other personaliz.	Reference number	None
Footer	Legal and company info	None
Story	Access to acc. restricted due to abnormal activities during last transaction	Credit card suspended due to unauthorized use
Call to action	Click link and enter account info to verify ownership	Fill credit card info into attached form and send back for verification
Additional info	Info about transaction	None
Priv./Sec. info	None	None
Attachment	None	Begrenzte_Kreditkarten_bilden.html (literal translation of restricted_creditcard_form)

Table 4: Features of Fraudulent E-mails Part 2

participants mentioned it at least once, and whether these results support the prediction. To control for possible learning effects, it shows the number of participants mentioning an aspect in the first e-mail and in the last e-mail they saw, respectively.

The "from" address was mentioned at least once by almost all participants. Most participants simply stated that certain "from" addresses appeared either authentic or dubious to them. Mostly the addresses in the fraudulent e-mails appeared dubious to participants because they were inconsistent with the signatory in the content, because they appeared unprofessional or came from an unexpected top-level domain. However, the cryptic appearance of the local parts of both the authentic Amazon and Facebook e-mails were mentioned as negative aspects by several participants as well. Link URL was also mentioned by a vast majority of participants. Most participants correctly identified the URLs in the fraudulent e-mail as suspicious because of domains which did not match the purported sender or lack of https and the URLs in authentic e-mails as trustworthy because of their domain names were known or at least fit the purported sender. However, the long cryptic link URL in the authentic Facebook e-mail was perceived as suspicious by some participants as well. Most of the mentions of subject lines were negative comments on the

Feature	Mentions	Part. Mentioning[a]	Supported?[b]
"From" Address	116	32 (12/17)	+++
Link URL	64	28 (7/10)	+++
Subject	7	6 (3/1)	+
Design / Layout	73	29 (6/6)	+++
Seal	12	10 (1/2)	+
Language	38	24 (4/5)	+++
Personalization	24	15 (2/2)	++
Signature / Comp. Info	17	12 (2/1)	+
Narrative Strength	24	17 (0/3)	++
Information / Cont. Quality	22	13 (4/4)	++
Context	40	28 (4/4)	+++
Persuasion Attempt	23	17 (1/3)	++
Privacy/Security Prot.	3	3 (0/0)	+
Reputation	1	1 (0/0)	-
Familiarity	31	21 (4/0)	++

[a] In brackets: Only mentions for the first/last email a participant has seen

[b] +++ : mentioned by most (24-34) participants, ++ : many (13-23) participants, + : few (2-12) participants, - : at most one participant

Table 5: Mentions of Factors Predicted to Influence Decision

subject of the e-mail about a blocked account, which was very simplistic and contained a capitalization error.

Another aspect mentioned by the vast majority of participants was design/layout. Missing design elements or bad layout were mostly mentioned as negative aspects of most of the fraudulent e-mails. The design of the Zalando e-mail with strong branding elements was mentioned as a positive aspect by many participants, but the design of the fraudulent "PayPal" e-mail was mentioned as a positive aspect by six participants as well, although three were suspicious about the authenticity of the logo. Mentions of trust seals were mostly concerning the presence of e-commerce trust seals as a positive aspect of the Zalando e-mail.

Language was mostly mentioned as negative aspects of most of the fraudulent e-mails due to their spelling and grammar mistakes and poor language in general, and as positive aspects of the authentic e-mails. The "personalization" category contains positive mentions of personal form of address or negative mentions of a lack thereof, as well positive mentions of the invoice number in the Amazon e-mail or the last digits of the account number in the comdirect e-mail. Mentions of the company information in the comdirect and Zalando e-mails, the lack of a personal signature and company information in the Visa/Mastercard e-mail and the mismatch between signatory name and sender address in the blocked account e-mail were categorized as "Signature / Company Information". The category "Narrative Strength" contains descriptions of e-mail content as (im)plausible, authentic/dubious, (not) making sense, but also explicit mentions that Visa and Mastercard are two different companies and therefore there cannot be an e-mail from both combined.

Comments about the amount and quality of general/supplemental information provided in e-mails was categorized as "Information / Content Quality". Especially the extensive information in the Zalando e-mail was praised by five participants, but also criticized by two. Three participants praised the information given in the purported PayPal e-mail.

Context was another aspect that the vast majority of participants mentioned at least once. That category consists mostly of participants mentioning that they would click the link in the Zalando e-mail or open the PDF attached to the Amazon e-mail if they had requested a password reset or placed the order mentioned, respectively. Four participants mentioned they would only go to the comdirect website if they had an account with them. The majority of the comments in the "Perceived Persuasion Attempt" category came from participants who either rejected the purported PayPal e-mail because it urged them to click a link and enter their login data (five participants), or who praised the comdirect or Amazon e-mails for being only informative in nature.

Of the three mentions of privacy/security protection, two are concerning the explanation of the privacy-preserving mechanisms in Amazon Marketplace's e-mail system, the third concerns the link to unsubscribe from notifications in the authentic Facebook e-mail. The only mention of reputation was one participant mentioning that she trusts Amazon. The last aspect which was predicted to influence decisions is familiarity with (receiving e-mails from) the sender. Comments in this category were from people who were cautious due to being unfamiliar with receiving that kind of e-mails from that sender (Amazon or Facebook), who trusted the Zalando e-mail because they recognized the logo from commercials, or who ignored or deleted e-mails because they have often received similar spam/phishing e-mails.

4.4 Exploratory Analysis

The analysis of the qualitative data found additional categories of aspects mentioned as affecting the decisions. Table 6 illustrates those additional aspects each with its total number of mentions and the number of participants mentioning it.

Aspect	**No. of Mentions Total**	**No. of Part. Mentioning**[a]
Encoding/Spaces	21	18 (3/3)
Time sent	7	6 (1/0)
Attachment	25	20 (1/4)
Advertisements	7	7 (2/0)
Limitation on Link	3	3 (0/0)
Curiosity	9	6 (1/0)
General Rule/Caution	81	31 (10/9)

[a] In brackets: Only mentions for the first/last email a participant has seen

Table 6: Frequencies of Additional Aspects Influencing Decisions

"Encoding/Spaces" refers to the encoding errors in the Visa/Mastercard e-mail and to the

missing spaces between some words in the account suspension e-mail, which participants mentioned as affecting credibility negatively. “Time sent” refers to participants finding the time at which the Visa/Mastercard e-mail was sent (midnight) suspicious. “Attachments” refers to participants mentioning either that they found the HTML file attached to the purported Visa/Mastercard mail to be suspicious or that the PDF receipt attached to the Amazon e-mail appeared either trustworthy or suspicious to them. Advertisements mostly refers to participants mentioning the advertisements in the password reset e-mail from Zalando as annoying and uncalled-for in this context, whereas the fact that the link for resetting the password was only valid for 24 hours (“Limitation on Link”) was mentioned as a positive aspect by three participants. If participants asked themselves questions like “Where will I get when I click the link?” and said they would click the link to find out, or if they indicated they would click the link and then investigate the site closely, or that they might click the link in the Facebook e-mail to see the news, those reasons were categorized as “Curiosity”. The category “General Rule/Caution” contains reasons like “I never read e-mails from Facebook”, “Banking is a delicate matter” or “A bank adviser would call me on the phone”. With 81 overall mentions and 31 out of 34 participants mentioning it at least once, General Rule/Caution turned out to be the second-most prominent category of reasons overall.

5 Discussion

All of the attributes of the message, sender or context that were predicted to influence the intention to follow a call to action contained in an e-mail were indeed mentioned by participants. The “from” address, design, link URL, context and language were the most prominent ones. The purported sender’s reputation, however, was mentioned only once, perceived privacy/security protection was mentioned only by three participants.

The prediction that the purported sender’s reputation affects the recipient’s trust and intention to follow a call to action was mostly derived from e-commerce literature, where reputation and brand have a large impact on willingness to purchase from a website. It could be argued that since the e-mails shown in this experiment were directed at existing customers, participants imagined they were existing customers of the purported senders. According to the two-stage model by McKnight et al. [MCK00], reputation only affects consumer’s trust in the early, exploratory phase and is displaced by actual usage experience afterwards. However, the results from this study still contradict previous studies in the phishing context [KAC06], where participants did indicate that the purported sender’s reputation/brand is important for their decision to trust them.

The fact that perceived privacy/security protection was mentioned only by three participants can be explained by the fact that the e-mails used here do not mention those protections in direct relation to the calls to action. They only contain links to unsubscribing from notifications (Facebook) or information about privacy and security protection in the e-mail system in general (Amazon). In this light, it is interesting to see that three participants still mentioned the general privacy-related information as contributing to their trust in the e-mail and/or its sender. The subject line was mentioned by only six participants.

This could be due to the fact that participants were directly presented with the full e-mail, whereas in reality, the subject line is more relevant before an e-mail has been opened, at least in e-mail clients which allow deleting an e-mail without viewing its body.

There were also reasons mentioned which were not predicted. While the encoding problems in one e-mail which were mentioned by many participants were specific to this particular e-mail, other reasons apply to other e-mails as well. The advertisements mentioned by seven participants as a negative aspect of the Zalando e-mail indicate that they did not expect an e-mail with a link to reset the account password to contain ads. The time when it was sent is another attribute which was not found to influence credibility of an e-mail before. Curiosity, which was interpreted as the reason behind the decision to click a link by six participants, was not found as a reason for following calls to action in previous studies, but Wainer et al. [WDK11] found it as an important factor for reading e-mails in general.

The most important unpredicted reason, however, was a general rule or caution. 31 of our 34 participants gave reasons in this category. That this was not found in previous studies can be explained by the fact that previous studies either focused on experimentally manipulated attributes of the e-mail, measured personality traits or asked participants for the reason why they thought an e-mail was authentic or not (which would not reveal general rules such as "I never read e-mails from Facebook" which relate to behavior, though they could have revealed rules such as "A bank adviser would call me on the phone"). These general rules may have been acquired through general anti-phishing education or from banks' explicit information to their customers (or, in the case of Facebook, result from the fact that users do not find these messages useful because they regularly log into Facebook anyway). Another reason mentioned by the majority of participants were attachments. Although previous quantitative phishing research has used e-mails with attachments as stimuli [DJCF07], we know of no study were they were mentioned by participants of qualitative studies.

Before discussing the implications of this study's results, its limitations of course have to be considered. First of all, this being a laboratory experiment, the situation participants were in differed from real-life e-mail reading situations in several aspects. Participants were observed both by the eye tracker camera and the experimenter while reading the e-mails, which may have put them under pressure to be extra careful (although they were not told that their task was to distinguish between authentic and fraudulent e-mails). The fact that even under these conditions, three out of 34 participants would have clicked the link in the e-mail purportedly from PayPal, however, indicates that participants were not overly cautious. Since participants were able to see the e-mail while being asked about what had led them to their reaction, they may have noticed features of it which they had not noticed before. Therefore, the importance of some aspects for user's decisions may be overestimated. This is particularly true for the link URL, which was always visible at the bottom of the e-mail, whereas in reality, it is only seen when the mouse cursor hovers over the link. To make the situation more realistic, actual HTML e-mails viewed in web browsers or e-mail clients will be used in future studies.

Seeing eight e-mails in succession could theoretically have introduced learning effects. As shown in tables 5 and 6, however, the number of mentions remained relatively stable be-

tween the first and last e-mail seen for most aspects. The only aspects being mentioned by disproportionately few participants for the first e-mail were narrative strength, persuasion attempt and attachment. Familiarity, on the other hand, was mentioned by disproportionately few participants for the last e-mail. Whether these results reflect actual learning effects has to be investigated in further studies. Another limitation to generalization is the composition of the sample. Although we were able to sample a relatively wide range of age and education groups, a majority of participants were still university students. Therefore, the sample is not representative of all e-mail users.

For these reasons, the actual proportion of successful attacks in this study should not be generalized to real-world proportions.

6 Conclusion and Outlook

Overall, the results from this study are largely in line with the model and thus with previous research. They show that recipients base their decision whether to follow a call to action contained in an e-mail on aspects of design, content, language, but also on more technical aspects like the "from" address, link URL or the time it was sent. The fact that the phishing e-mail that purported to come from PayPal tricked three of our participants into believing it was authentic and clicking the link to enter their account data demonstrates that even in 2013, a phishing e-mail which is well written, contains graphical elements from the original brand and presents a convincing narrative can still be dangerous.

Providing users with general rules such as "A bank will never ask you for account details via e-mail" is confirmed to be effective in protecting them from at least some phishing attacks. Apparently, banks have been more effective than PayPal in teaching their customers such rules, and the results from this study emphasize the importance of improving their risk communication efforts.

Apart from general rules, another important result is that either users should be taught to pay less attention to design aspects or that the design elements should be hidden by default when displaying e-mails from unknown addresses or with other automatically identifiable suspicious attributes (which some e-mail clients already do) to prevent them from distracting users from more reliable indicators of authenticity.

The fact that context played a major role in participants' trust decisions emphasizes the danger of spear phishing [WHC+12], which abuses this reliance on context by targeting recipients based on information gathered on the web (for example finding out the e-mail address of an ebay user who is bidding on an auction which is about to end and sending him or her an e-mail about that auction). It therefore has to be communicated to e-mail users that a fitting context does not guarantee that an e-mail is authentic.

The central contribution of this study to research in this area is demonstrating that the question participants are asked can limit or enhance the insights gained from their answers. General rules or curiosity as reasons for why users do or don't follow calls to action in e-mails cannot be found when asking users to decide whether an e-mail is authentic or fraudulent and give reasons for that decision. This should be kept in mind whenever open

questions seek to find new reasons instead of just confirming known ones.

With interviews as its main method, this study was well-suited to focus on the aspects of the message which influence the recipient's decision. Other aspects of the model such as personality traits or knowledge and experience have to be evaluated in quantitative studies. A further iteration of the study presented in this paper could aim for improved generalizability by putting participants in a situation which is closer to real life. However, a potential bias caused by participants' reflection on their own thought processes – which is necessary for qualitative studies – can never be completely avoided.

Acknowledgements We thank the anonymous reviewers for their helpful comments, although unfortunately some of them could not be implemented due to space limitations.

References

[DJCF07] Ronald C Dodge Jr, Curtis Carver, and Aaron J Ferguson. Phishing for user security awareness. *Computers & Security*, 26(1):73–80, 2007.

[KAC06] Ponnurangam Kumaraguru, Alessandro Acquisti, and Lorrie Faith Cranor. Trust modelling for online transactions: a phishing scenario. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, PST '06, pages 11:1–11:9, New York, NY, USA, 2006. ACM.

[MCK00] D. Harrison McKnight, Vivek Choudhury, and Charles Kacmar. Trust in e-commerce vendors: a two-stage model. In *Proceedings of the twenty first international conference on Information systems*, ICIS '00, page 532–536, Atlanta, GA, USA, 2000. Association for Information Systems.

[PTK13] Thomas Pfeiffer, Heike Theuerling, and Michaela Kauer. Click Me If You Can! – How do users decide whether to follow a call to action in an online message? In Louis Marinos and Ioannis Askoxylakis, editors, *Human Aspects of Information Security, Privacy, and Trust*, number 8030 in Lecture Notes in Computer Science, pages 155–166. Springer Berlin Heidelberg, January 2013.

[SW11] Frank Stajano and Paul Wilson. Understanding scam victims: seven principles for systems security. *Communications of the ACM*, 54(3):70–75, 2011.

[WDK11] J. Wainer, L. Dabbish, and R. Kraut. Should I open this email?: inbox-level cues, curiosity and attention to email. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, page 3439–3448, 2011.

[WHC+12] Jingguo Wang, T. Herath, Rui Chen, A. Vishwanath, and H.R. Rao. Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication*, 55(4):345 –362, December 2012.