Adopting the CMU/APWG Anti-Phishing Landing Page idea for Germany

Melanie Volkamer, Simon Stockhardt, Steffen Bartsch, Michaela Kauer
SecUSO, Computer Science Department, CASED, Technische Universität Darmstadt
Darmstadt, Germany
[firstname.surname]@cased.de

This work has been published in the Third Workshop on Socio-Technical Aspects in Security and Trust (STAST) 2013 DOI: 10.1109/STAST.2013.12

***Abstract*—Phishing attacks still pose a significant problem and purely technical solutions cannot solve this problem. While research literature in general shows that educating users in security is hard, the Anti-Phishing Landing Page proposed by CMU researchers seems promising as it appears in the most teachable moment – namely once someone clicked on a link and was very likely to fall for phishing. While this page is already in use and exists in many languages we show that it is not effective in Germany as most users leave the page immediately without having read any advice. We therefore explore options to adopt their ideas for Germany. We focus on which are the trustworthy institutes that could provide such a landing page on their web pages and what is an appropriate headline and design.**

Keywords—phishing education; trust;

I. INTRODUCTION

Phishing attacks are still a big problem as statistics on successful attacks [1] and user studies [2] show. This is not surprising as attacks become harder to detect for users. Spelling and grammar mistakes in the messages become less common and the messages are increasingly personalized based on knowledge from the web – in particular from social network platforms. Moreover, attackers use in addition to e-mail further services for their phishing attacks like SMS, social network posts, or instant messaging.

Of course, the security mechanisms likewise improved in detecting phishing messages and web pages. However, the mechanisms are not able to catch all phishing – particularly not immediately after the phishing has been initiated. Those they detect are taken down with the consequence that users who try to visit the page (by clicking on a link in a corresponding message) see a 404 error page. This means we have currently three groups of users on the Internet: (1) Users who fall for phishing because the phishing web pages have not yet been taken down. They lose money or have other types of negative consequences. (2) Users who click on the link and see a 404 error page. They are confused and have usually no idea what happens and what the problem is. (3) Users who detect that this is a phishing attack and thus either do not click on the link or do not enter their credentials on a phishing page.

Kumaraguru et al. [3] proposed the idea of using the "most teachable moment" to educate the second group of users and thereby reducing the number of people who fall for phishing (group 1). This most teachable moment is when users have just clicked on a link in a phishing message. Therefore the authors introduced the phishing-education landing page which the user sees instead of the 404 error page. This landing page (see Figure 1) has been developed with focus groups. It is provided by the Anti-Phishing Working Group and Cylab as part of their APWG/CMU Phishing Education Landing Page program[1].

Fig. 1: Anti-Phishing Landing Page[2]

[1] http://education.apwg.org/education-redirect-program/

[2] http://phish-education.apwg.org/r/en/?www.phishsite.com/the-phishing-page.html, http://phish-education.apwg.org/r/de/?www.phishsite.com/the-phishing-page.html (German version).

This work has been published in Proceedings of the Third workshop on Socio-Technical Aspects in Security and Trust (STAST) (p./pp. 46-52): IEEE Computer Society, DOI: http://dx.doi.org/10.1109/STAST.2013.12

As this web page exists in many languages including German and some German phishing links are also redirected to this page, we decided to test the effectiveness of the information provided on this page with German citizens. Therefore, we set up a lab study telling the participants that we intend to study how they treat the massive amount of emails one is confronted with in daily life. However, most of the participants left the phishing landing page immediately (close browser/tab or click the back button) and without having read any information on this web page. Therefore, we investigated on how to make Germans stay on such a page, in particular long enough to read the provided information carefully. We used an explorative approach (while taking the comments from the users of our original study into account) and improved the relevant components of such a page iteratively over five studies. We could show that the institution BSI (German Federal Office for Information Security) is the most effective institution of the ones tested. Moreover, evaluating the original webpage design providing the anti-phishing information shows that also the web page of the BSI is the most effective one. The headline "Security Warning" is most effective within the headline options we evaluated.

II. Landing-Page Effectivness Study

The Anti-Phishing Landing Page intuitively is a good idea and according to learning theory a very promising approach. We wanted to know whether the way it is implemented is effective for German citizens. We define effectiveness by the fact that people who are redirected to the Anti-Phishing Landing Page (1) stay there and read the necessary information carefully enough; and (2) are able to identify phishing e-mails and phishing web pages. In addition, the goal was to identify shortcomings with the current page.

A. Methodology

The evaluation was conducted as lab study. The participants were told that we study their behavior wrt. different types of e-mail messages. There were some pre-conditions the participants had to fulfill include that they have an amazon account. One e-mail was a phishing email and by clicking on the link participants were redirected to the German Anti-Phishing Landing Page.

The whole study was divided in four phases: (1) pre-questionnaire, (2) dealing with the emails in the inbox while thinking aloud, (3) questionnaire regarding the Anti-Phishing Landing Page, (4) quiz on different potential phishing emails and webpages. Those participants who did not click on the link in the phishing email because they already are aware of it being a phishing email were asked to click on the link at the end of phase (2) in order to enable them to answer the questions in phase (3). 32 people participated; 44% female; the average age was 30 years while the oldest participant was 65 and the youngest 19 years old.

B. Results

We were in particular interested in the reaction to the Anti-Phishing Landing Page: 8 participants left the page immediately; 15 had a very quick look but were unsettled by the term 'Warning' and the many different components and thus also immediately left the page without reading anything else than 'Warning'; 4 were unsettled first but then start reading and understood that it is an education page; for 5 participants it was very soon clear that it is an education page.

In the third phase we asked open questions to collect detailed information about shortcomings of this page (note, those who immediately left the page were asked to go there again and have a look). The most important comments were:

- Unclear, confusing, too much information and pictures at once;
- Irritation by the owl;
- General more appropriate for children: type of pictures, fish and owl;
- Unknown institutions on top of the page;
- Some mentioned the background color.

As we expected that people had doubts about the (for them unknown) institutions Cylab and APWG we also included a question who should provide such a page. The answers were mostly very abstract like trustworthy institutes. However, seven mentioned 'governmental institutions' and six mentioned 'known companies' (examples include Microsoft, Google, and anti-virus software developers). For the same reason we also asked how they think phishing education would be most effective. Besides an improved Anti-Phishing Landing page, half of them propose newspapers and TV and six proposed webpages from banks, shops, and email providers. Three proposed tutorials by internet providers, schools, universities, and employers.

We also asked whether people feel safe for future potential phishing emails / web pages after having read this page carefully. 72% agreed on this. Unfortunately we did not ask why. We assume that there is a relation to the trust issues they had at the beginning when deciding to leave the page immediately. In the quiz (phase 3) only 4 participants were able to properly distinguish between phishing and non-phishing emails and web pages. The best results got those examples on which similar indicators could be found as those indicators discussed on the Anti-Phishing Landing Page.

We conclude that the existing Anti-Phishing Landing Pages are not effective enough for German citizens because 23 of our 32 participants (72%) immediately left the page without reading and because only 4 were afterwards able to properly distinguish between phishing and non-phishing emails and web pages. In this paper we focus on the first challenge namely to design the web page in a way that people stay on this page and read enough to understand the situation and to decide whether they want to know more about phishing and how to protect themselves.

III. Re-Designing the Anti-Phishing Landing Page for German Citizens

We used an explorative approach (while taking the comments from the users of the first study into account) in

order to re-design this education page towards a more effective approach for Germany. We conducted an iterative approach over five user studies. Our main focus is on the institution which should provide such a page and the headline because those two aspects seemed to be the most important aspects for the participants to decide whether to stay on the landing page or not. The goal is to come up with a new design and show that people are much more likely to stay and read the education hints. As the main study design remains the same over the five studies, we first describe the general study design and then the approaches we tested in each round.

A. General Study Design

The study is divided in five parts. (1) Participants are first confronted with the following situation: They are shown a printout of an email from amazon with a link. Then, we asked them how they would behave if the following page would open while showing a printout of one of the tested re-designed pages (depending on to which group of web pages the particular participant is assigned to). We distinguish between would read carefully, would scan and leave afterwards, and would leave immediately. We also ask to justify their decision.

(2) Afterwards, we measure the first impression based on a semantic differential and therefore are ask the participants (while the web page they just saw is covered again) to fill out a table with seven adjectives pairs and five different parameter values. The adjectives are: well-arranged/ confusing, up to date/ old fashioned, clear/ unclear, reliable/ unreliable, comprehensible/ incomprehensible, safe/ dangerous, easy/ complex.

(3) In the third part, after de-briefing the participants concerning the purpose of the study, they conduct a small card sorting experiment of different design options. While sorting they were asked to think aloud about the reasons for their decision. They get printouts of different re-designed pages (while only the institute changes) and are asked to sort them depending on how likely this page would cause them to stay on the web page and read further. (4) Afterwards, they got a new set of re-designed pages to sort while this time the pages only differed with respect to the headline. (5) The study closes with questions on demographics (age, gender, and education).

We decided not to conduct this test as lab test with real emails and web pages as this is more effort and harder to get participants. For the purpose of this explorative approach we accepted the drawbacks of our design. However, the final design will be tested in either a lab or a field study to avoid any concerns on validity.

Note, the study was conducted and evaluated in German and for the purpose of this paper relevant phrases were translated.

We asked different participants for all the conducted studies. The demographics are provided in Table 1 for each of the conducted studies.

We chose to recruit all 60 participants via convenience sample method from the University cantina. 49 Participants have the "Abitur" which is the German equivalent to A-level. Seven participants that took part in our studies had the advanced technical certificate which is another entrance qualification for university. Four participants had a secondary school leaving qualification and were either university employees or people who work around the university.

Table 1 Demographics

Study	**f/m**	**avg. Age**	**Education (A-level Y/N)**
First four landing page versions	7/13	33	15/5
Amazon as additional institute and two more headlines	2/3	25	5/0
Amazon with the original web page layout	3/2	25	3/2
Amazon without advertisements	2/3	25	5/0
Different pages with original web page design	9/16	25	16/9
Total	23/37	28	49/11

B. First four landing page versions and their evaluation

The focus is on the selection on institutes and the headline which cause people who click on a link and are forwarded to re-designed landing page are highly likely to stay and read. For the institutes we selected the following ones:

- Federal Office for Information Security[3] (BSI), as a representative of a governmental institution as mentioned by the participants in the study evaluating the existing page. Note, even if the institute itself might not be well known but in the logo they have the German eagle as in the German flag and the colors from the German flag.
- 'Verbraucherzentrale'[4] (VZ) - the Federation of German Consumer Organizations, as a representative of a non-governmental institution which is known from news to take care about the consumer rights both in the real world but also on the Internet.
- A banner of many known, large companies, as companies were also mentioned in the evaluating study. We took the banner from SiN (Deutschland sicher im Netz e.V.[5]) an initiative to make an active contribution to greater IT security in Germany to which the corresponding companies and associations contribute.
- TÜV Süd[6], as it has been shown earlier in the context of seals for web shops that this is the seal which is best known and people trust in most [4]. In addition people know this logo from the regular checks required for their car but also for other engines like elevators.

[3] https://www.bsi.bund.de/EN/Home/home_node.html
[4] http://www.verbraucherzentrale.de/en/index.php
[5] www.sicher-im-netz.de
[6] http://www.tuev-sued.de/home_en

The different logos we used are shown in Figure 2. We decided to start with a simple common design and not with the design of the web pages of the corresponding institutes in order to avoid interception by the design of these different web pages.

Fig. 2: Anti-Phishing Landing Page

For the headline we selected the following once:

- Security warning
- Security advice/ hint (in German: Sicherheitshinweis)
- Consumer warning
- Consumer advice/ hint (in German: Verbraucher-hinweis)

The idea is that security warning is rather strong and maybe even to strong. In order to weaken the headline we decided to test also advice/hint instead of warning (note actually advice also fits more to the purpose of this page) and also consumer instead of security. Here the motivation was that this pages addresses actually consumers. However, it might be that consumer advice/hint is not strong enough or does not sound important enough. The goal was to see which provide the best balance.

For the first phase of the study we decided to test the 4 different institutes but stick to only one headline namely security advice/hint. The first test was conducted with 20 participants, i.e. 5 in each group for phase (1) and (2) and 20 for the questions/tasks in phase (3), (4), and (5).

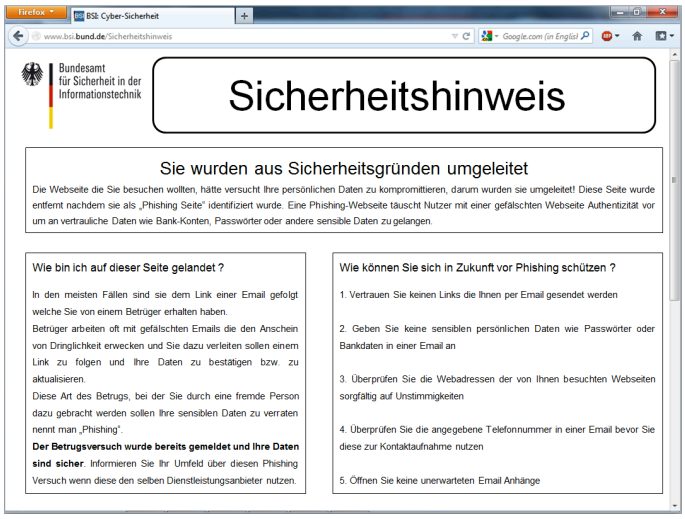

Fig. 3: Example page for BSI and security advice/hint as headline

The result of phase (1) with respect to the institutes is: BSI (3-2-0[7]) performed best wrt. remaining long enough on the landing page, then TÜV Süd (2-3-0), then SiN (2-0-3) and then VZ (0-2-3).

This is supported by the semantic differential (phase (2)) and the ranking in the card sorting part (phase (3)) for BSI and TÜV Süd: the semantic differential is 2,69 for BSI, 2,91 for TÜV Süd. The average ranking over all 20 participants for BSI is 1,45 (while 1 is the best one) and for TÜV Süd is 2,15.

The semantic differential and the ranking in the card sorting part is slightly better for VZ (3,4) than for SiN (3,57) and also in the ranking VZ got better results (2,75) than SiN (3,65).

With respect to the reasons for deciding to leave or stay as well as for the rankings the following comments are worth mentioning:

- 2 of the 5 participants in the BSI group and 4 of the other groups during sorting the different pages mentioned as reason the German eagle.
- Reasons for leaving mentioned on several pages: too much text, no trust in this page, no motivation
- In total 4 out of the 6 participants who immediately left the page stated that they have expected to see Amazon.
- During the ranking 2 mentioned that the TÜV Süd Logo is well known, 6 did not like the design with the VZ logo and 6 mentioned that they do not trust the SiN one as it looks like advertisement.

The result with respect to the different headlines from the ranking in phase (4) is: Security Warning (2,05) performs best, then Consumer Warning (2,4), then Security Advice/Hint (2,6), and then Consumer Advice/Hint (2,95).

While this is exactly the order in which we also defined those terms, one must be careful with the result as the numbers

[7] In brackets we provide the numbers for would read carefully, would scan and leave afterwards, and would leave immediately.

are very close together. This is also supported by the comments participants made. 5 participants stated that Consumer * in particular the combination Consumer Advice/Hint is not motivating while other 5 participants stated that Security * and in particular Security Warning is too strong and would cause them to be afraid and thus immediately leave a corresponding page.

C. *Evaluating Amazon as additional institute and two more headlines*

Based on the results, we decided to also test Amazon as a possible institute. Note, Amazon would be what participants expect to see if they click on the link. However, this would mean that there is not one Anti-Phishing Landing Page to which everyone is redirected but if the link referred to the web provider X than this link would need to be redirected to an Anti-Phishing Landing Page on web provider X's web pages. While this is much more difficult to realize if possible at all we wanted to evaluate whether this would be more effective than the other four we evaluated in the first study.

We also decided to include more headlines in the card sorting task in phase (4), namely,

- just "Warning" as in the first study both terms containing the term "Warning" performed best; and
- "Security and Consumer Warning" to address the fact that people made comments in both directions for Security Warnings and Consumer Warnings.

The study design was the same as described in subsection A. Correspondingly, we also asked 5 people to participate. The printout of the page in phase (1) contained the Amazon logo and the headline Security Advice /Hint.

The results of phase (1) for the Amazon group with respect to the question whether people would remain and read is: 2-1-2; thus actually worse than BSI and TÜV Süd.

The same also holds for the semantic differential which is 3,11 for Amazon and was 2,69 for BSI and 2,91 for TÜV Süd.

Being less effective than BSI and TÜV Süd is also supported by the values of the ranking for these 5 participants which is TÜV Süd 1,8, BSI 2,0, Amazon 2,2, VZ 4,2, and SiN 4,8. The only comment we got was about the design of the page namely that it does not look like Amazon pages usually look like. Note, it is not too surprising that no one stated something similar before for any of the other institutes as the participants probably new the institutes but not how their web pages look like.

The ranking of the pages with the different headlines shows that at least for these 5 participants the best one is still Security Warning; and the newly tested ones are almost the worst once. The only one that is worse is Consumer Warning.

D. *Evaluating Amazon with the origininal web page layout*

Due to the comments regarding the design, we wanted to evaluate whether using the proper Amazon web page design improves the effectiveness (see Figure 4 for the corresponding page we evaluated). According to the Amazon web page design, the headlines were written in orange.

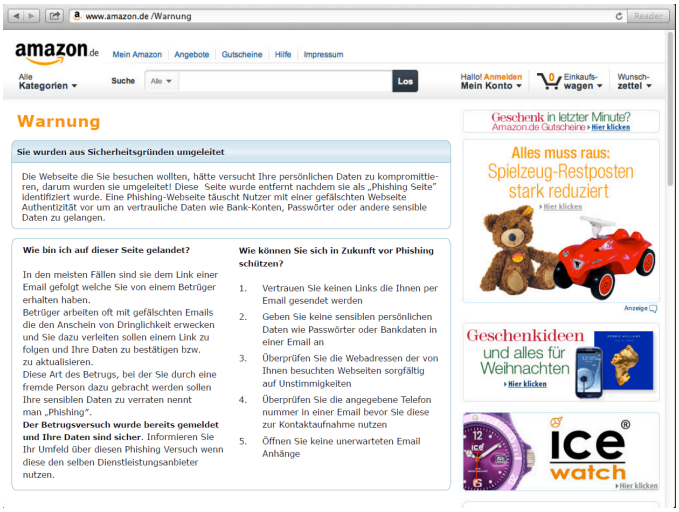

Fig. 4: Example page for Amazon with the design from Dec. 26th 2012

The results of phase (1) for the Amazon group with respect to the question whether people would remain and read is: 3-2-0; thus better than without adopting the design and as good as the BSI approach in the first run. The semantic differential is even lower than with the BSI approach, namely 2,51.

However, in the ranking the BSI approach performs better (1,8) than the Amazon one (2,2) – but still better than TÜV Süd (2,6).

The only comment we got from two of the participants was that the page looks not really reliable due to the huge amount of advertisements. Thus, in total using the design of the Amazon page has a positive effect.

The ranking of the pages with the different headlines was combined with the results from the previous subsection. According to these 10 participants the order is: Security Warning (2,4), then Warning (3,1), then Security Advice/Hint (3,3), then Consumer Advice/Hint (3,8), then Consumer Warning (3,9), and then Security and Consumer Warning (5,1). Thus still the best one is Security Warning.

E. *Evaluating Amazon without advertisements*

Due to the comments regarding the advertisements, we decided to evaluate whether using this type of Amazon web page improves the effectiveness further. We also removed the menu bar as we were afraid that people who reach this page may stay but not read the advices but just click on login or in general use Amazon as usual. Then the education would also not effective maybe even the approach would encourage people to click on links and then continue using such pages by logging in. See Figure 5 for the corresponding page we evaluated.

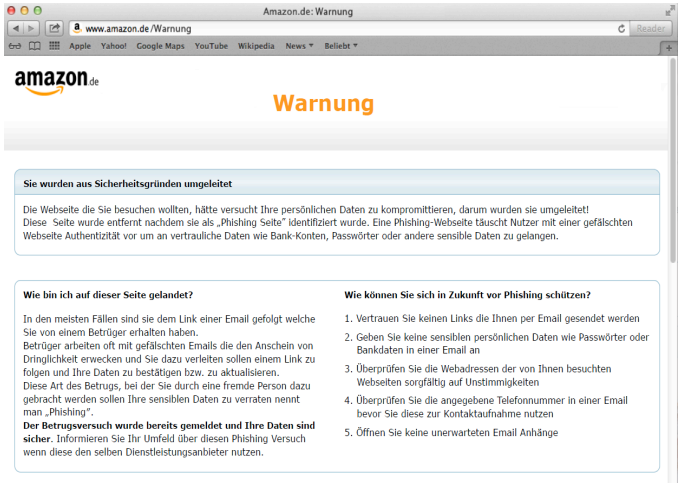

Fig. 5: Example page for Amazon without advertisements

The results of phase (1) for the Amazon group with respect to the question whether people would remain and read is: 3-2-0; thus the same as before. The semantic differential (2,6) is almost the same as with the advertisements (2,51). However, in the ranking, this Amazon page performs better (1,8) then the BSI approach (2,0). Note, we compare a designed page with the one from the first test just containing the logo of the corresponding institutes. Note further, the ranking for the other institutes is always the same: BSI, TÜV Süd, VZ, SiN.

The only comment we got from two of the participants was that the page looks not really reliable due to the huge amount of advertisements. Thus, in total using the design of the Amazon page has a positive effect.

The ranking of the pages with the different headlines was combined with the results from the previous subsection. According to these 15 participants the order is: Security Warning (2,2), then Security Advice/Hint (2,7), then Warning (3,5), then Consumer Advice/Hint (4,0), then Consumer Warning (4,2), and then Security and Consumer Warning (4,7). Thus still the best one over all 15 participants is Security Warning. Thus, in the following study we use this headline.

F. Evaluating different pages with original web page design

Due to the fact that the comparison in the previous two subsections between the different institutions is not fair (only Amazon was tested with the real design of Amazon web pages), we decided to run a final test on the institutions where all web pages are designed according to the real webpages. This is also necessary to see whether the design of the other institutions web page has an influence to the overall result.

Based on the results from the previous studies we only tested Amazon, BSI, and TÜV Süd, as well as only the headline Security Warning. Furthermore, we only tested phase (1), (2), (3), and (5). Note, as BSI and TÜV Süd run to different web pages, we included both in this study (BSI and BSI für den Bürger[8] and TÜV Süd and TÜV 2[9]). The corresponding pages are shown in Figure 6 to 8.

Fig. 6: Example page for a landing page in BSI design

The results of phase (1) is: BSI (5-0-0), BSI für den Bürger (1-3-1), Amazon (2-1-2), TÜV Süd (4-0-1) TÜV 2 (3-0-1). The result of phase (2) is: BSI (2,14), BSI für den Bürger (2,63), Amazon (2,43), TÜV Süd (2,26), and TÜV 2 (2,71). For the ranking in phase (3) the result is: BSI, BSI für den Bürger, TÜV Süd, TÜV 2, and Amazon.

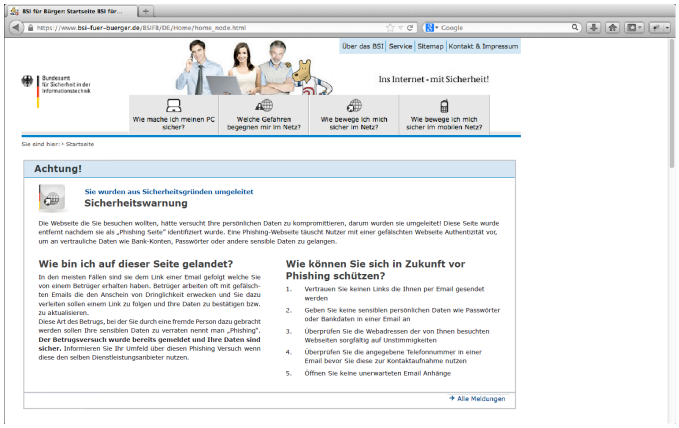

Fig. 7: Example page for a landing page in BSI "für den Bürger" design

[8] The BSI für den Bürger web page is a web page prepared by the BSI for German citizens providing general and understandable advices for secure behavior on the Internet. The BSI page is the one about the institute itself.

[9] The TÜV Süd page itself is the more general one about the institute while the TÜV Süd Safe Shopping webpages focuses on Internet concerns and in particular on the evaluation they conduct on online web shops.

Fig. 8: Example page for a landing page in TÜV Süd design

Fig. 9: Example page for a landing page in TÜV 2 design

Thus, over all conducted studies, BSI seems to be the most trustworthy institution and the most promising webpage to cause people to stay on this page seems to be the one of the institution and not the one prepared for the citizens. Note, even if only five participants saw each page as the first page they were all asked to rank them. Correspondingly, 25 participants in this study ranked the BSI page.

IV. Conclusion and Future Work

User studies and successful phishing attacks show that phishing is still a big problem. As phishers use new channels and the messages become increasingly professional and personalized, it is not enough to rely on technical solutions but also increase awareness. We believe that the Anti-Phishing Landing Page approach proposed by Cranor et al. is in general a plausible way to educate users about security issues on the Internet because it uses the most teachable moment – the moment one clicked on a recent phishing link – to educate people about phishing and how they can protect themselves. As the used Anti-Phishing Landing Page was designed within focus groups of North American participants it was unclear how effectively the page would protect and help Internet users in other countries or cultures. We evaluated its effectiveness within a lab user study in Germany and showed that it is not effective here in its current state. The findings of this study also show that the user interface affects the willingness of users to access security advice and in particular that it is important that they trust the provided information, including the institution providing the information. As this is relevant for any type of security education, more research in this area is desirable.

Afterwards we explored options for a new design of such an Anti-Phishing Landing Page specifically for Germany. We improved the design iteratively and conclude that a governmental institution – the BSI (Federal Office for Information Security) – seems to be the most promising institution. Furthermore as the most promising headline we identified the phrase "Security Warning". While these results are very promising, it is only a solution for Germany and due to the German flag also very specific for Germany. It is also unclear whether similar institutions exist in other countries or whether there is a Europe-wide institution which people know and trust. The latter approach would have the advantage that it is not necessary to have different landing pages for each individual country.

There is another shortcoming of our findings and proposals: The findings about trustworthy institutions also support adversaries. They can exploit the trustworthiness of the institution to improve their attacks and, indeed, this has already been done by virus programmers who blocked the user's screen, requiring the victims to pay a particular amount of money in order to get the computer unblocked. The virus stated to be a message from the federal German police. However, this is a general problem; compare proposing approaches to better remember passwords (e.g. first letters from sentences). Therefore, it might be time for a general maybe even philosophical discussion about such relations.

As a next step we plan to conduct focus groups to design the body of the page. Here we plan to work on the text below the headline and the other sub headlines. We plan to reduce the content one can see at first. Further information like how to protect against phishing might only be displayed after having clicked on the corresponding sub headlines. While most of our study participants were highly educated, we plan to recruit participants with more diverse demographics (age groups, backgrounds and education levels) for our focus groups. In particular, we plan to work with those who do not know what phishing is and how protect themselves.

After the design, we will work on the text. In particular we will distinguish between the different applications that phishers uses nowadays, like email, SMS, instant messaging, and messages in online social networks. We also plan to integrate the text and the design of such a page in a second approach namely displaying the information by the web browser in a warning style blocking dialog. This is of particular interest because existing phishing warnings have been shown to be less effective (compare e.g. results in [5]).

Finally we will run again a lab study or, if possible, a field test to evaluate the effectiveness of the final Germany-specific Anti-Phishing Landing Page and in particular compare it with the APWG one and the browser warning style one.

References

[1] RSA: Phishing Attacks Net $687m to Date in 2012 http://threatpost.com/rsa-phishing-attacks-net-687m-date-2012-082412/ [visited 4-28-2013]

[2] Study: Half of Users Can't Recognize Phishing (from 2012) http://channelnomics.com/2012/08/30/study-users-recognize-phishing/ [visited 4-28-2013]

[3] Kumaraguru, Cranor, Mather: Anti-Phishing Landing Page: Turning a 404 into a Teachable Moment for End Users. Whitepaper: http://docs.apwg.org/reports/APWGLandingPage-Turning404intoEducation.pdf

[4] Volkamer, Karayumak, Kauer, Halim, Bruder. Security versus Trust Indicators in 2011 in Germany. In 5th MPICC Interdisciplinary Conference on Current Issues in IT Security 2012. Duncker & Humblot

[5] Egelman, Cranor, Hong: You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings, In Proceedings of the CHI 2008 Conference on Human Factors in Computing Systems, 2008.

ACKNOWDLEDGEMENT

We would like to thank Henning Stecher and Markus Hau for their support in preparing and conducting the studies.