Can We Fight Social Engineering Attacks By Social Means? Assessing Social Salience as a Means to Improve Phish Detection

James Nicholson

PaCT Lab
Northumbria University
Newcastle upon Tyne, UK
james.nicholson@northumbria.ac.uk

Lynne Coventry

PaCT Lab
Northumbria University
Newcastle upon Tyne, UK
lynne.coventry@northumbria.ac.uk

Pam Briggs

PaCT Lab
Northumbria University
Newcastle upon Tyne, UK
p.briggs@northumbria.ac.uk

ABSTRACT

Phishing continues to be a problem for both individuals and organisations, with billions of dollars lost every year. We propose the use of nudges – more specifically social saliency nudges – that aim to highlight important information to the user when evaluating emails. We used Signal Detection Theory to assess the effects of both sender saliency (highlighting important fields from the sender) and receiver saliency (showing numbers of other users in receipt of the same email). Sender saliency improved phish detection but did not introduce any unwanted response bias. Users were asked to rate their confidence in their own judgements and these confidence scores were poorly calibrated with actual performance, particularly for phishing (as opposed to genuine) emails. We also examined the role of impulsive behaviour on phish detection, concluding that those who score highly on dysfunctional impulsivity are less likely to detect the presence of phishing emails.

1. INTRODUCTION

Phishing is a highly prevalent form of social engineering where an attacker steals sensitive information by sending fraudulent emails that purport to be from a trustworthy source. Over time, phishing attacks have become both socially and contextually smarter, with the result that phishing continues to be a growing problem for organisations and individuals. In the best-case scenario, phishing results in lost productivity due to users deliberating over the authenticity of the email, but in the worst-case scenario individuals and businesses can suffer serious security, financial and/or reputation loss due to stolen credentials or leaked information.

A large number of people fall for these phishing emails within experimental studies [25, 31, 38]. For example, McAfee's Phishing Quiz [31] found that 80% of respondents (employees) fell for at least one phishing email – an alarmingly high percentage. A recent "in the wild" study showed that users do not only follow the link, they go on to provide their credentials to the website. This study, by Bursztein et al. [6], examined the effectiveness of phishing websites by analysing internet traffic through Google, and found that the most successful phishing web page resulted in 45% of page views converting into captured user credentials. However, not all webpage visits successfully converted to captured credentials, while an average conversion rate of 14% was found across all the websites they looked at. To deal with this issue, researchers have focused on two core strategies: either improving the filtering algorithms that can reduce the number of phishing emails that make it into users' inboxes (e.g. [3, 9]) or developing interventions, mainly training and education, that help users identify fraudulent emails (e.g. [40]). Despite these efforts, both individuals and organisations continue to fall for phishing scams and billions of dollars are lost every year – the Monthly Online Fraud Report for January 2015 estimates losses of over $4.5 billion for 2014 [37].

In the current study, we focus on the second of these strategies, exploring interventions that might support the user in the detection of fraudulent emails. In particular, we wanted to explore the effect of making the broader social context of the email more salient. We did this firstly by highlighting the name of the sender along with the time the email was sent, recognising that genuine emails are typically exchanged during certain social or business hours; and secondly, by highlighting the number of people in an organisation or network that received that same email, recognising that genuine emails are targeted at specific individuals or groups, while phishing emails are more socially indiscriminate.

2. Background Research

As we have noted, attempts to deal with the phishing problem embrace both technical and human-centric solutions. Technical solutions have generally focused on identifying suspicious websites, for example using browser plugins or identifying characteristic elements of a phishing email, e.g. [16]. Filtering algorithms can also bring improvements, e.g., [3, 9], however such phishing tools are not always accurate – some phish are missed and some genuine items are flagged as phish, i.e. there are problems with false positives and negatives [50].

The human-centric solutions typically fall into one of three categories involving (i) educational or training interventions; (ii) new designs and visualisations that can help 'nudge' users to make better decisions and (iii) work that considers individual differences in decision-making. Our work primarily addresses the latter two categories, but we will briefly consider some of the educational initiatives below.

2.1 Campaigns and Educational Interventions

Users are unlikely to take effective action against phishing attacks unless they are both aware of the risks inherent in online communication and are also knowledgeable about the specific threats posed by dubious emails. Indeed, researchers have shown that the perceived risk of cybercrime can moderate users' willingness to take risks in a variety of online environments [36] and that the ability to evaluate deceptive cues was a major factor in online protection [22]. Further, users' cybersecurity (i.e., phishing) knowledge is positively related to their attitude and intention toward adopting and using cybersecurity (anti-phishing) solutions [46]. It is unsurprising, then, that a number of educational interventions designed to improve user understanding of risk and knowledge of how to mitigate risk have been developed. These interventions adopt a wide range of different training techniques that can include embedded training systems [28] motivational cartoons [29] and even games that raise awareness and train users for future encounters [41]. However, they have been met with limited success. Users start with a very poor awareness of their vulnerability to being phished [23, 46] and may ignore the training altogether [8]. Added to that, the phishing emails become more sophisticated year on year - to the point where even security experts are unable to determine whether the item is genuine or not [18].

2.2 Behavioural Interventions

When seeking to influence user behaviour, we must be mindful that people are reluctant to spend much time and effort engaging in protective privacy or security measures [24, 39]. Many cybersecurity interventions are unproductive and unhelpful in the sense that they take time and effort away from the users' primary task. This productivity argument is important, as employers often do not appreciate how much time is lost due to staff deliberating the legitimacy of emails. Of course, the costs to organisations can be much worse when employees get this wrong and when companies are then laid open to serious cybersecurity threats and can incur significant financial and/or reputation loss.

However, we should also be aware of the vulnerabilities exhibited by users during the regular processes of communicating by email. Ferreira et al., [20] note that the principle of Liking, Similarity & Deception (LSD) rules in this context – as people simply tend to believe in what others do or say as a default, unless they have good reason to suspect something is really wrong or they find a particular behaviour is completely unexpected. With this in mind, many researchers have turned to the principles derived from behavioural economics in order to design a range of seamless cybersecurity "nudges" (see [43]) or visualisations [10, 11] that help move the user away from this default position, so that they make better choices, but choices that do not require too much additional effort on their part. Behavioural nudges are already popular in the privacy field, with successful examples being found in relation to reduced Facebook sharing [47] and improved smartphone privacy settings [1]. They are also becoming popular as cybersecurity interventions, e.g. in relation to the risks associated with the selection and installation of apps on mobile phones [10]. For phishing, the existing interventions typically seek to make the trustworthiness of the linked webpage more salient within the web browser. For example, Chou et al. [12] proposed SpoofGuard, a toolbar that gave pages a *Spoof Score* to help the user evaluate the likelihood that the page is not genuine. This score is based on a URL check (whether URL appears to be genuine), an image check that includes logos (e.g. detecting that an eBay logo does not sit on a non-eBay.com domain), a link check (check that all links in the page point to the current or same domain), and a password check (if page requires password, then more scrutiny is needed). An experimental system called CATINA [51] employed such an approach to obtain a 97% accuracy rate in recognising the phishing websites it examined, with a 6% false positive rate. However, these technical approaches rely on a page being reported as a phishing site before they can be used. Other interventions have explored the effectiveness of browser warnings, including toolbars. This work has generally found warnings and toolbars ineffective (e.g. [48]) – in part due to the user ignoring them. However, further work exploring the design of the phishing warnings on browsers found that active warnings – those requiring an action from the user to be dismissed – were clearly more effective than passive warnings [17].

Other behavioural interventions have focused upon email attachments, which pose a known security problem [14]. Polymorphic Dialogs have been proposed for opening email attachments where, for example, the order of the options might change regularly in order to prevent habituation (or automatic skipping), and a timer can be introduced that forces the user to study and evaluate other options [5]. However, unsurprisingly, such interventions can significantly increase the time taken to complete simple tasks – again, resulting in unacceptable productivity costs for the end user [2].

There have not been many interventions to support the user in detecting the phishing emails themselves within the email client. The aforementioned Polymorphic Dialogue [5] is an example of an intervention built into the email client to deal with attachments, while PhishDuck [49] is another example of a client-based extension designed to deal with phishing links. When a suspicious link is clicked by users, PhishDuck displays a popup asking for confirmation of the action, and presents a suggestion that they may have intended to use a different link (e.g. paypal.com instead of paipal.com). A user study found that participants using the extension followed significantly less phishing links than those using the default email client warning message.

Some email providers and clients will present warnings to users when discrepancies are detected. For example, Gmail displays a banner warning on the top of a message if the email claims to be from a Gmail address but has not been authenticated as such [44] and while this can be a very useful indicator, it only applies to emails from the same domain. The Mozilla Thunderbird email client also displays a banner warning at the top of the email message when (internal) discrepancies are identified [45], but also incorporates the use of a pop up warning requiring the user to click on a continue button if they click on any links within the message. Once again, this fall-back system relies on the automated detection of features within the message that earlier spoofed the spam filter. Finally, it is possible to set up Microsoft Outlook so that users are not able to click on links within emails, but must instead copy and paste (or retype) the URL directly into the web browser. However, this does not attempt to assess if the email is a potential phish and may result in non-discriminatory behaviour from the user to minimise productivity disruption.

2.3 Individual Differences in Susceptibility to Attacks

We already know something about the kinds of people likely to be most vulnerable in a phishing attack. For example, females are more prone than males to misclassifying phishing emails as

genuine [25, 26, 29, 40]. Halevi et al. [23] found a relationship between neuroticism and susceptibility to phishing attacks and various work has found that extroverts, more trusting individuals, and those open to new experiences were more vulnerable to phishing attacks [25, 33]. In contrast, Pattinson et al. [35] reported that extraverts and individuals scoring high for openness managed phishing emails better, which they acknowledge as a counter-intuitive finding, but also reported a marginal effect of impulsivity, with those scoring high for impulsivity showing greater susceptibility to phishing attacks, while Modic and Lea [33] hint at an effect of impulsivity by reporting that Premeditation (an item of their impulsivity scale) was the best predictor for scam response rate in their scam compliance survey. Finally, in a recent study of attitudes and behaviours online, Riek et al. [36] have also found an interesting relationship between user confidence, risk perception and the use of online services. Specifically, more confident users have a higher chance of becoming victimized, although they are also more able to identify cybercriminal attacks. This is in contrast with other work in phishing where a positive relationship has been reported between performance (identification) and confidence [7].

In the current study, we have tried to explore nudges that can alert the user to the possible presence of a phishing email. These are simple visual cues that build upon the social premise of a phishing attack – wherein a user is socially engineered to believe that the email comes from a genuine source (e.g. because the sender is known or the content of the email seems appropriate). However, we go further in providing cues that make the social context of the sender more salient (highlighting the name and address of the sender, and the time the email was sent) and the social context of the recipient more salient (highlighting the number of other recipients of that email). We loosely based our two nudges on existing work from other security and privacy contexts, notably installation dialogues that highlight the vendor's name [4] for the former and audience saliency from social media work [47] for the latter (see Section 3.1 for full details).

We hypothesise that each of these should improve phish detection, but we also explore individual differences in user susceptibility to phishing emails, by measuring both functional and dysfunctional impulsivity [13] and user confidence in their own cybersecurity decision-making.

3. Methodology

In order to determine the effectiveness of the two nudges, we set up an online experiment via Amazon's Mechanical Turk where participants were asked to view 18 emails (6 phishing, 12 real) and decide whether each email represented a genuine message or a phishing message. The emails were designed by the researchers but were modelled on real messages received within the previous 3 months. The phishing emails, specifically, were faithful reproductions of emails that had been problematic (as reported by the I.T. department) within the university during that time period.

3.1 Design

The study had a 2 x 2 independent measures design. The first factor, *sender saliency*, was created by highlighting sender features on the email that included name, email address and the time the email was received. This factor had two levels (highlighted, not highlighted). It was chosen, in part, to exploit the social nature of a phishing attack where senders may seem familiar [16] but in all likelihood, the normal "social hours" of that sender would be understood (e.g. it would be unusual to receive an email from a colleague or from a

local organisation at 1am). Although the name of the sender can be spoofed, it is common of phishing emails to contain discrepancies between the name of the sender and the original email address. In essence, the sender saliency nudge also aimed to expose any discrepancies in the address field of the emails thereby reducing the likelihood that users would be lured into a false sense of trust. This nudge was modelled on similar security work on installation dialogues showing that highlighting the vendor's details to direct users' attention to potential discrepancies led to more secure behaviour [4]. The sender saliency nudge could be easily deployed in an organisation or to individual users through an email client plug in or using a browser extension.

The second factor, *receiver saliency* was created by informing the user of the number of people within their organisation that also received a version of the email. Again, there were two levels of this factor (receiver information present or absent). This factor was designed to exploit the social context of emails, in that genuine emails are constructed for a particular audience or individual, whereas a spear phishing email from a compromised account may be sent to multiple unrelated recipients. Whilst we recognise that mass emails from popular services (e.g. PayPal) may be sent to multiple recipients, the content or *lure* often appears to be highly personal "Ms x, your account may have been compromised, so please click here to change your password"). If a user is alerted to the fact that a seemingly personal message has been sent to many colleagues, they may question the validity of that message. The converse may also be true – i.e. if they receive a message that should, by its nature, have been distributed to whole organisation (e.g. using a standard mailing list) and yet they are the sole recipient, then again, they may re-evaluate the legitimacy of that message. This nudge was loosely based on the Picture Nudge [47] on Facebook demonstrating that unintended information disclosure could be minimised by alerting the users to the post's target audience. In our case, we have reversed the paradigm where the user instead gets a visual measure of the message's intended audience. The likely deployment of the receiver saliency nudge would be in an organisation where email data can be easily collected to inform the nudge's numerical output.

3.2 Participants

A Human Intelligence Task (HIT) was posted on Amazon's Mechanical Turk (MTurk) stating that we were looking for users willing to help out with an email-sorting task. Participants were given a flat fee of $0.45 for completing the task which had an average completion time of 10 minutes, mirroring the payment structure of other studies at the time. The inclusion criteria for taking part in the study were a minimum age of 18, a good level of English, and a Number of HITs Approved greater than or equal to 50 (for quality purposes). Participants on mobile devices were excluded from participating to control the viewing experience of the emails.

We set recruitment targets based on an *a priori* power analysis suggesting 279 participants for a medium effect, with a final sample of 281 participants then completing the task to the required standard (see Table 1 for details). No attention checks were employed in the experiment, but the data provided was inspected for validity in terms of the time spent on the task: The work from workers who spent two or less seconds on average per email was rejected and new workers were found to complete the study. Participants were randomly allocated to one of the four groups (sender salience cue present/absent; receiver salience cue present/absent).

Nudge	N	Mean Age	F	M	U
None (Control)	65	34.5	29	34	2
Sender	64	35.7	31	32	1
Receiver	79	31.7	31	45	3
Combined	73	32.3	20	52	1
Total	281	33.6	111	163	7

3.3 Materials

The 18 emails were presented to participants as static images, with 6 designed as the target phishing emails and the remaining 12 as genuine (see Appendix A.1). Phishing emails were (loosely) matched with genuine emails in terms of the time of day they were received and the percentages of colleagues flagged as also receiving the messages (receiver saliency nudge). This was done by matching six of the genuine emails with the features of the phishing emails (i.e. similar time of day they were received) while the remaining 6 were chosen to reflect the overall established patterns of that set (e.g. most emails received during working hours). Note that this approach is rather conservative, in that we are deliberately reducing the simple effectiveness of our time of day cue as a signal of whether emails are genuine or not, but we are operating on the assumption that some genuine emails may reasonably be received at night (e.g. emails from another continent) and that by alerting users to time sent, we are encouraging them to check the other aspects of the email more carefully.
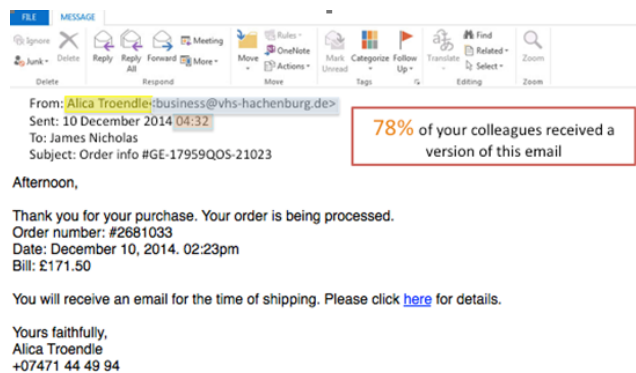

Figure 1: Example phishing email showing both nudges – sender (highlights left) and receiver (box right).

All messages were placed under an image of the Microsoft Outlook Ribbon bar (see Figure 1) to provide a frame of reference to participants. The "to" field in each email was edited to show *James Nicholas* as the receiver and any personal or identifiable information within the email body was edited with generic information.

The emails chosen for this study covered a basic range of possible senders and were matched across phishing and genuine messages: emails from well-known providers (e.g. Amazon, PayPal, eBay), emails from smaller organisations (Spotify, Eversure) and emails from individuals. We chose emails that contained links to websites as these are the most common type of phishing attack by volume

[42] although in practice the nudges should work in the same manner with emails containing attachments.

The website was hosted on our own server but the recruitment was facilitated through Amazon's Mechanical Turk.

We note that the phishing emails, modelled on problematic phishing emails received within the university, were designed to always present a cue as to their authenticity to overcome the limitation of having no active links: when the sender metadata (to/from/subject) did not show a clear discrepancy to allow an informed choice, the links in the body of the message were not masked or obscured (similar to previous work [7]).

3.4 Measures

The main dependent variable was whether the user classified each email as either genuine or a phish. This was a binary decision, but the time taken to make a decision (in seconds) on each email was also recorded, starting when the page loaded and concluding when the radio button for the decision was pressed. Finally, participants were asked to rate how confident they were with their own classification of the email as genuine or phish, using a drop-down menu with options ranging from 0% to 100% confident in increments of 10%.

In addition, participants were asked to complete an impulsiveness personality questionnaire at the end. Impulsiveness has been linked with susceptibility to phishing emails in previous work (e.g. [28, 35]). Despite weak associations, the trends reported are interesting enough to warrant further exploration of this aspect of personality in our study. We used a reduced version of Dickman's Impulsivity Inventory [13] and the final scale consisted of 6 items measuring functional impulsivity (acting without much forethought, to maximise efficiency), with an internal reliability of 0.670 (Cronbach's Alpha) and 6 dysfunctional impulsivity items (acting without much forethought, but with undesirable consequences), with an internal reliability of 0.856.

3.5 Procedure

The experiment was initially framed as an email-sorting task on the MTurk HIT, but once participants clicked through to the homepage of the study, they were given more specific instructions telling them they would be required to identify phishing emails. This initial deception was put in place to prevent the recruitment of individuals only interested in computer security. Once on the website, they were randomly assigned to one of the four experimental groups and given the task instructions: they must look through 18 emails that were received by a person called James Nicholas and classify the message as either a genuine email or as a phishing email. After each decision, participants then provided a confidence score for their decision and progressed to the next message. Once all messages had been classified they were thanked and given a code to enter on the Mechanical Turk page. Participants received their payment once their work was reviewed by the research team.

4. Results

4.1 Scoring

The absolute user judgement of genuine/phish was scored in terms of classical signal detection theory, i.e. as a hit, a miss, a true negative or a false positive. In our task, *hit rate* refers to phishing emails that were correctly identified as phishing emails. *False positive rate* (or false alarms) refers to genuine emails that were incorrectly identified as phishing. Signal detection theory was

developed to determine the sensitivity of a participant to the presence of a target (phishing emails) against a background of noise (genuine emails). The discriminability index *d'* is a statistic used in signal detection that provides the separation between the means of the signal and the noise distributions in units of standard deviation of noise distributions. *d'* was calculated using the equation:

$$d' = Z(phish\ hit\ rate) - Z(false\ positive\ rate)$$

Bias in decision-making (i.e. whether users tend to classify things as phish or as genuine, irrespective of accuracy) is measured via the Beta statistic (β). Beta, is a statistic that provides a measurement of the extent to which one response is more probable than another and is calculated using the equation:

$$\beta = exp\{d' \times C\},\ where\ C = \vartheta - \{d'/2\}$$

The two other measures generated by our design (and used in the calculation of Beta) are *Miss Rate* – referring to phishing emails that were identified as genuine emails and *True Rejection Rate* – genuine emails that were identified as such by the participant. We refer readers to relevant texts (e.g. [7, 32]) for further information on this method.

4.2 Sensitivity to Phishing Emails

We ran three independent t-tests on the sensitivity (*d'*) scores, comparing the control (no nudge) condition with the other experimental conditions (sender saliency nudge, receiver saliency nudge, and combined nudges). Means for d' in each condition are presented in Table 2.

Table 2: Sensitivity *d'* (higher is better) for each nudging condition (range: -4.53 - 4.53).

Nudge	N	Mean (*d'*)
None (Control)	65	0.59
Sender	64	0.98
Receiver	79	0.87
Combined	73	0.92
Total	281	0.79

These planned comparisons revealed a significant improvement in phish detection (*d'*) when sender saliency cues were employed (*t(127)=2.080, p=.020*) but no significant difference when receiver saliency cues were employed (*t(142)=1.498, p=.068*). We also found improved performance against the control when the cues were combined, i.e. when both sender and receiver salience cues were present (*t(142)=1.667, p=.049*). An additional t-test between the sender saliency and the receiver saliency cues reported no significant differences between the two (*t(141)=.598, p=.551*).

4.3 Bias

We compared the bias (β) score for each nudging condition against the control to determine whether the nudges influenced the likelihood of participants to respond "phish" or "genuine" irrespective of what was actually presented. Means for β can be seen on Table 3.

Table 3: Bias β (low = tendency to select "phish", high = tendency to select "genuine").

Nudge	N	Mean (β)
None (Control)	65	1.90
Sender	64	1.47
Receiver	79	1.87
Combined	73	1.65
Total	281	1.73

Again, planned independent t-tests were made of the experimental conditions against the control. There were no statistically significant differences when comparing the sender saliency condition (*t(127)=1.439, p=.153*), the receiver saliency condition (*t(142)=0.100, p=.920*), or the combined cues conditions (*t(136)=0.773, p=.441*) against the control. Thus, the improved detection performance for sender salience and combined conditions noted above were not associated with any change in the participants' bias in terms of a tendency to classify emails as phish or as genuine.

4.4 Decision Time

While participants' sensitivity to phishing emails and their bias were the main variables under investigation, the time taken to make each decision was considered important in the light of the drive towards productive security solutions. The time taken to decide on individual emails ranged from 3 seconds to 117 seconds, with a mode of 9 seconds. We note that only 1.3% of decisions were made in 3 seconds, evenly spread across participants. Table 4 presents the mean number of seconds required to select a response per email.

Table 4: Average time taken to make a decision on an email (seconds per email).

Nudge	N	Mean (*seconds*)
None (Control)	65	19.91
Sender	64	20.28
Receiver	79	18.18
Combined	73	18.79
Total	281	19.22

We found no significant difference in time taken to make a decision when comparing each of the experimental conditions against the control, i.e. no difference for sender salience (*t(127)=0.208, p=.836*), for receiver salience (*t(142)=0.975, p=.331*), or for the combined condition (*t(136)=0.725, p=.470*). Thus, the improvements in detection accuracy, presented above, do not incur a time penalty and should not lead to productivity losses.

4.5 Calibration of Confidence

We noted earlier the importance of well calibrated confidence in making risk decisions. In this study, we measured user confidence in each email judgment and mean confidence ratings are given in Table 5, below.
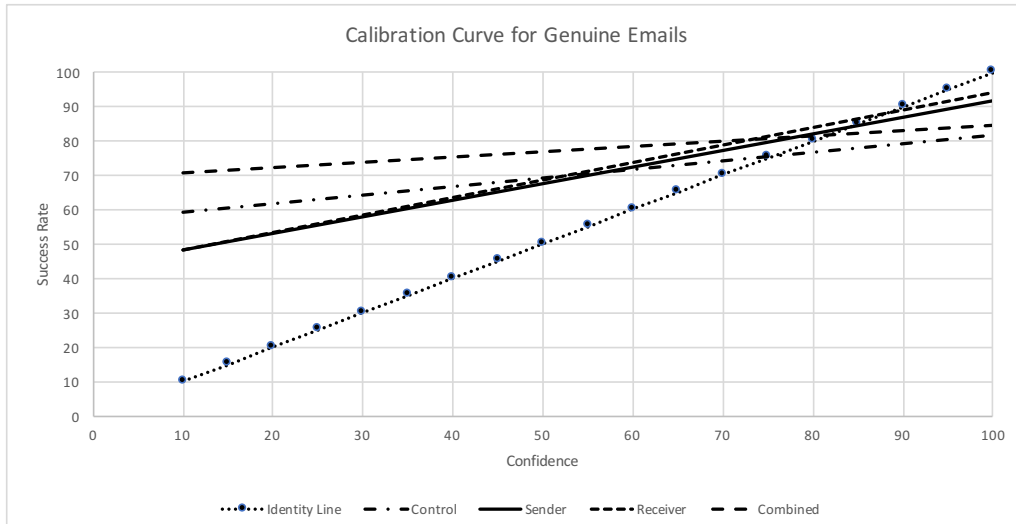
Figure 2: Calibration Curve for genuine emails. The identity line shows perfect calibration with underconfident responses plotted above and underconfident responses plotted below.

Table 5: Confidence (%) indicated by participants per choice.

Nudge	N	Mean (%)
None (Control)	65	68.24
Sender	64	69.63
Receiver	79	69.89
Combined	73	67.12
Total	281	68.73

We then constructed confidence calibration curves for both the phishing and the genuine emails. A calibration curve is a graph where subjective confidence of being correct is plotted against the actual performance (in this case percentage confidence is measured against percentage accuracy). The curves are created by computing the mean accuracy of those items where participants have given a particular confidence score. On each figure, the diagonal or *identity*

line shows perfect calibration. Any data points above this line show *under-confidence* and points below the line show *over-confidence*. To take one example, a data point that shows 80% on the x-axis and 40% on the y-axis is showing that when we aggregate those emails in which the mean confidence rating is 80%, the mean accuracy rate for those same emails is only 40% (i.e. participants are over-confident). Thus good calibration would be indicated by data curves forming close to the diagonal or identity line and poor calibration would be shown by deviation from this line [30].

If we look firstly at the calibration curves for genuine emails (Figure 2) then we can see that under-confidence predominates – users are generally more accurate than they believe themselves to be. However, there appears to be a linear trend, suggesting that greater confidence is generally associated with better accuracy and there is some suggestion that the two 'nudges' of cueing sender and receiver salience can act to improve calibration of confidence.

Turning now to the calibration curves for phishing emails (Figure 3) then we can see how poorly calibrated user confidence is for
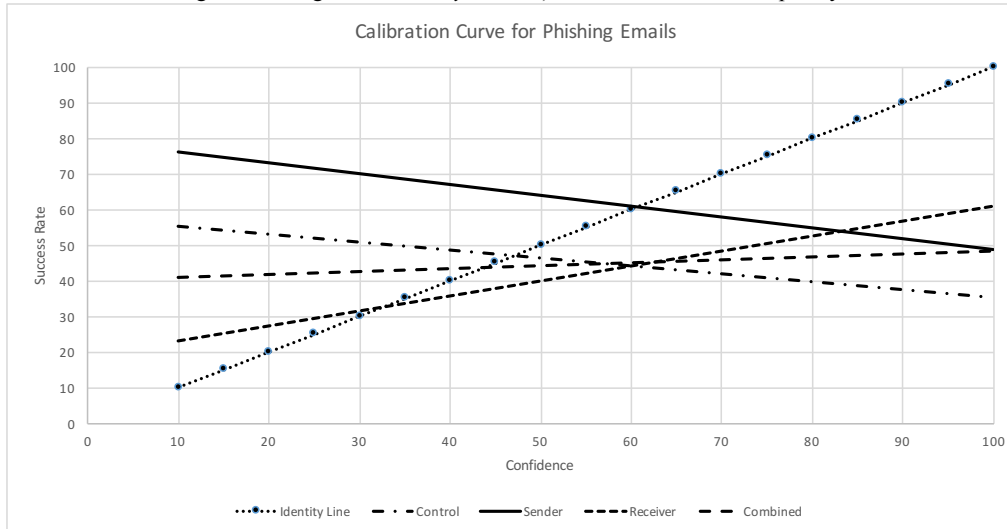

Figure 3: Calibration Curve for phishing emails. The identity line shows perfect calibration with underconfident responses plotted above and underconfident responses plotted below.

these items – with no overall sense that users are sensitive to their own ability to detect phish. The improvements in phish detection that gave rise to the significant d' score in the sender salience condition is reflected here in the solid line being associated with higher accuracy rates, but what is fascinating is that the cue that gives rise to improved accuracy cannot be harnessed to give users a better sense of how well they are doing in making this judgment.

4.6 Impulsivity

We used the scores on the Dickman scales to identify the top and bottom quartiles for both functional and dysfunctional impulsivity (i.e. we created four groups with approximately 60 participants per group and used the top scoring and bottom scoring groups for the analysis while discarding the middle two groups). We then conducted t-tests to compare these groups and found no significant effect of functional impulsivity (again taking d' as the measure of phishing sensitivity) ($t(157)=1.348, p=.179$). However, for the dysfunctional trait we found a significant difference in sensitivity to phishing emails between high and low scorers ($t(142)=2.987, p=.003$) where participants who scored high in dysfunctional impulsivity were relatively poor at detecting phish ($d'=0.62$) when compared to those with those who scored low on the trait ($d'=1.13$).

These findings beg the question of whether or not the different nudges we have designed would be particularly effective as "protective measures" for those with dysfunctional impulsivity, but here we hit an analysis problem as we have not controlled for dysfunctional impulsivity in our allocation of participants to groups and so have a variable distribution of 'dysfunctional impulsives' across cells compounded by a relatively low n which makes us reluctant to undertake an inferential analysis. For completeness, however, we give the sensitivity scores (d') and standard deviations for each of the conditions in Table 6, below.

Table 6: Phishing sensitivity (d') by condition for high and low impulsives.

Nudge	N	High dysfunctional impulsivity d' (s.d.)	N	Low dysfunctional impulsivity d' (s.d.)
None (Control)	14	0.15 (0.97)	12	0.67 (1.08)
Sender	15	0.98 (1.17)	11	1.12 (0.63)
Receiver	16	0.58 (1.25)	15	1.60 (1.07)
Combined	19	0.79 (1.21)	21	1.19 (1.44)

Finally, we found a significant difference between those scoring high vs. low on dysfunctional impulsivity on the time taken to make decisions, using a non-parametric Mann Whitney U test due to the non-normal distribution of data ($U=1803.5, p<0.01$). High dysfunctional impulsives made faster decisions on average (mean = 15.90s) than low dysfunctional impulsives (mean = 18.27s).

5. Discussion

The purpose of this study was to evaluate whether we can use the social context of sending and receiving emails to improve participants' ability to detect phish. We highlighted information about either sender (name, email address, and the time the email was sent) or receiver (number of people in the organisation who received the email) as two means of *nudging* people to think more carefully about the communicative context of the email. These two nudges individually and in combination were tested against a control where users were simply shown the email in its original, non-altered format.

We found that improving sender saliency led to better phish detection when compared with a control and that sender and receiver nudges used in combination also improved performance, although there was no real sense of any added value from the receiver nudge. The improvements were not associated with any overall bias in terms of participants' inclination to decide "phish" or "genuine". We also found that participants were under-confident in their decisions when presented with genuine emails, but were over-confident when presented with phishing emails. Finally, we found that participants who scored high on the trait of dysfunctional impulsivity [13] were less accurate in identifying phishing emails and made faster decisions than those scoring low for the trait. These results are discussed in more detail below.

5.1 Performance with Nudges

The sender saliency nudge presented alone and in combination with a receiver saliency nudge improved phish detection over the control condition. In other words, the simple act of highlighting fields that are already present in an email – sender's name, email address and time sent – was an effective means of improving user security – a finding that is consistent with other work that suggests persuading users to attend to such information can help users with phish identification [16]. Users already rate these features as important for identifying phishing emails, with 95% of lay participants reporting that they use the "from" field to pick out discrepancies between email and sender name [15]. However, it seems that this knowledge is not being applied in practice – even under those circumstances where participants had been instructed to look for phishing emails. We should also note that the email address field is by default hidden in several popular email clients. For example, on Gmail's web interface a user is required to hover over the sender's name in order to bring up the email address (after a few seconds' delay), and in Microsoft Outlook the user has to perform a number of steps in order to be able to see the origin email address. These practices are unlikely to help users in spotting discrepancies in emails and should be avoided.

Our results show that participants using the receiver saliency nudge (i.e. indicating how many other people were in receipt of the email) did not perform significantly better than participants viewing the email without nudges (control). It is possible that the wording used for the receiver saliency condition – highlighting the percentage of "colleagues" who also received the email – was not descriptive enough for participants, and a more detailed approach similar to that employed by Wang et al. [47] where specific individuals are named may work better. However, the privacy implications of such an implementation in an organisation should first be considered.

We did not find any associated effect on bias (i.e. participants were no more likely to select "phish" overall when nudged, irrespective of whether the email was or was not genuine). This is important, as nudges that simply make people more or less conservative overall (without improving sensitivity) could have unfortunate consequences, leading to either the rejection of genuine emails or the acceptance of fraudulent emails.

5.2 Confidence in Phish Detection

Parsons et al. [34] have shown that participants are more accurate at identifying phishing emails when they know they are taking part in a phishing experiment. However, our participants were rather poor at phish detection, and more worrying, were not well

calibrated in terms of the confidence they placed in their own judgements, further supporting previous work emphasising the importance of self-confidence when identifying phishing emails [7]. In other words, there was a discrepancy between subjective confidence and objective performance when classifying emails and this discrepancy seemed particularly problematic for phishing emails, where participants were generally poor at detecting phish (i.e. showed lower accuracy levels) but were overconfident that they made the right decision. On the other hand, for genuine emails, participants showed better calibration in confidence scores, although showed an overall pattern of under-confidence. This finding is interesting and is probably worth pursuing further. It is conceivable that users employ different cues for the detection of genuine emails than they do for the detection of phish but we would need to explore this issue in future studies. For the moment, we might note that good calibration of confidence essentially depends on both the amount and the strength of the evidence available in supporting the choice [27]. For phish decisions, users have relatively poor sources of evidence available and this is likely to be compounded by their inability to assess the quality of that evidence.

5.3 Impulsivity and Phish Detection
Previous work has suggested that impulsivity may play a role in phish detection. For instance, less impulsive people have been found to manage email better (i.e. spot phishing more efficiently) than those scoring high for the trait, based on the Cognitive Reflection Task [35]. It should be noted, however, that this result pertained to participants who were aware that they were taking part in a phishing task (i.e. were vigilant). Kumaraguru et al. [28] also found a trend where participants with lower Cognitive Reflective Task scores (i.e. with higher impulsivity) were more likely to click on phishing emails, although in this case the trend was not statistically significant.

Our results are consistent with these findings, but here we have used Dickman's distinction between functional and dysfunctional impulsivity, finding that only the dysfunctional scale is associated with poor phish detection. What is encouraging, is that our sender saliency intervention would appear to be effective even for those with low impulsivity (Table 5) however we have been reluctant to conduct any inferential statistics on these data as the power would be rather low, given the relatively small cell sizes and of course we have not systematically controlled for levels of impulsivity across the intervention conditions.

5.4 The Use of Signal Detection Theory in Phishing Research
In the past, phishing research and email classification in general typically analysed results using separate measures for success rate and false positives (e.g. [40]) or simply an accuracy measurement (e.g. [14, 19, 21, 28, 35]). This results in a simple ratio that indicates how comfortable users are identifying phish but neglects false alarms (i.e. incorrectly classifying a genuine email as a phish). Yet false alarms are becoming a concern for organisations as they are associated with productivity and/or business losses that arise when staff ignore legitimate emails. Additionally, simple measures of success that ignore decision bias are also problematic as changing the tendency to classify emails as phish or genuine irrespective of their actual legitimacy is not the target outcome.

Signal detection theory accounts for both false positives and response bias with the two main measures of sensitivity (d') and bias (β). We have shown in this paper how applying this analysis method teases out intricate performance measures that may be missed when using other methods. We are aware of two other papers that have recently utilised signal detection theory in phish detection [7, 34]. Canfield et al. [7] found that participants were accurate in determining the correct action for phishing emails (deleting or marking as "spam"), but that their sensitivity to phishing emails was poor. Parsons et al. [34] found that participants aware of their participation in phishing experiments were more sensitive to the phishing emails.

We are pleased that this measure is being adopted in phishing research, given how important the separation of sensitivity and bias are for realistic interventions in phishing.

5.5 Limitations
Although we were able to obtain a number of interesting insights from the study, there are two main limitations that we should discuss that may have affected the performance of participants.

Firstly, the messages used for both phishing and genuine emails were not actually received by the participants, thus it is unclear how familiar they were with each email. For example, it is possible that some participants may be familiar with the receipt of Amazon emails, direct from the retailer. They could then have used this knowledge to help them pick up subtle cues to aid their decision making. Whereas other participants may be unfamiliar with Amazon and as a result be at a disadvantage when judging the veracity of emails. This is a common pitfall with lab-based phishing experiments and can be addressed by running "in the wild" studies, although these introduce other limitations.

Secondly, participants were unable to interact directly with the email messages or carry out any additional checks (e.g. search for the company online). We addressed this issue by always having visible cues to allow informed decisions (see Section 3.3 for details).

Finally, participants were told from the beginning that they were taking part in a phishing experiment. These instructions will have primed them to scrutinise each email more closely than perhaps they would do otherwise [34]. However, given that all participants in all conditions were subjected to these instructions then this should not have affected our main findings – i.e. the effects should be the same for all. We note that, overall, our participants may have shown better sensitivity to phish than those who receive fraudulent emails "in the wild". Unfortunately, we cannot compare our findings with any normative data as sensitivity estimates are not available elsewhere.

6. Conclusions
In this paper, we evaluated two nudges with the aim of improving users' phishing detection on email clients. We found that users were more successful identifying phishing emails when their attention was drawn to the sender's details (name and originating email address) and the time received when compared with the control condition. This is problematic, given the recent design trend on popular email clients to hide important sender information (i.e. the full originating email address) by default, thus potentially hindering users' efforts when evaluating emails in their everyday lives. We also found strong evidence that individuals scoring high for dysfunctional impulsivity were at a disadvantage when identifying phishing emails and set this finding against previous published work which has been inconclusive about the effect of impulsive behaviour on phishing

identification (e.g. [28, 35]). We noted an interesting finding in relationship to users' overconfidence when making decisions in respect of phishing emails (and underconfidence in respect of genuine emails) and we would encourage further research in this area. Finally, we would recommend the adoption of Signal Detection Theory for phishing research, in particular due to the response bias measure that allows further scrutiny of potential interventions.

7. ACKNOWLEDGMENTS

8. REFERENCES

[1]   Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F. and Agarwal, Y. 2015. Your Location has been Shared 5,398 Times! *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15* (New York, New York, USA, 2015), 787–796.

[2]   Beautement, A., Sasse, M.A. and Wonham, M. 2008. The compliance budget. *Proceedings of the 2008 workshop on New security paradigms - NSPW '08* (New York, New York, USA, Aug. 2008), 47.

[3]   Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G. and Strobel, S. 2010. New filtering approaches for phishing email. *Journal of Computer Security*. 18, 1 (Jan. 2010), 7–35.

[4]   Bravo-Lillo, C., Komanduri, S., Cranor, L.F., Reeder, R.W., Sleeper, M., Downs, J. and Schechter, S. 2013. Your attention please. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13* (New York, New York, USA, 2013), 1.

[5]   Brustoloni, J.C. and Villamar'\in-Salomón, R. 2007. Improving security decisions with polymorphic and audited dialogs. *Proceedings of the 3rd symposium on Usable privacy and security*. (2007), 76–85.

[6]   Bursztein, E., Margolis, D., Archer, A., Pitsillidis, A. and Savage, S. 2014. Handcrafted Fraud and Extortion : Manual Account Hijacking in the Wild. *In Proceedings of the 2014 Conference on Internet Measurement Conference* (2014), 347–358.

[7]   Canfield, C.I., Fischhoff, B. and Davis, A. 2016. Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors: The Journal of the Human Factors and Ergonomics Society*. 58, 8 (2016), 1158–1172.

[8]   Caputo, D.D., Pfleeger, S.L., Freeman, J.D. and Johnson, M.E. 2014. Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*. 12, 1 (Jan. 2014), 28–38.

[9]   Chandrasekaran, M., Narayanan, K. and Upadhyaya, S. 2006. Phishing E-mail Detection Based on Structural Properties. *NYS Cyber Security Conference* (2006), 1–7.

[10]   Chen, J., Gates, C.S., Li, N. and Proctor, R.W. 2015. Influence of Risk/Safety Information Framing on Android App-Installation Decisions. *Journal of Cognitive Engineering and Decision Making*. 9, 2 (Jun. 2015), 149–168.

[11]   Choe, E.K., Jung, J., Lee, B. and Fisher, K. 2013. Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing. Springer Berlin Heidelberg. 74–91.

[12]   Chou, N., Ledesma, R., Teraguchi, Y. and Mitchell, J.C. 2004. Client-side defense against web-based identity theft. *Most*. (2004), 1–16.

[13]   Dickman, S.J. 1990. Functional and dysfunctional impulsivity: personality and cognitive correlates. *Journal of personality and social psychology*. 58, 1 (Jan. 1990), 95–102.

[14]   Dodge, R.C., Carver, C. and Ferguson, A.J. 2007. Phishing for user security awareness. *Computers & Security*. 26, 1 (2007), 73–80.

[15]   Downs, J.S., Holbrook, M.B. and Cranor, L.F. 2006. Decision strategies and susceptibility to phishing. *Proceedings of the second symposium on Usable privacy and security - SOUPS '06* (New York, New York, USA, 2006), 79.

[16]   Drake, C.E., Oliver, J.J. and Koontz, E.J. 2004. Anatomy of a Phishing Email. *Proceedings of the First Conference on E-mail and Anti-Spam (CEAS)* (2004), 1–8.

[17]   Egelman, S., Cranor, L.F. and Hong, J. 2008. You've been warned. *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08* (New York, New York, USA, 2008), 1065.

[18]   Even security experts fail to spot phishing emails, finds report: 2015. .

[19]   Ferguson, A.J. 2005. Fostering e-mail security awareness: The West Point carronade. *Educase Quarterly*. 28, 1 (2005), 54–57.

[20]   Ferreira, A., Coventry, L. and Lenzini, G. 2015. Principles of persuasion in social engineering and their use in phishing. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2015), 36–47.

[21]   Furnell, S. 2007. Phishing: can we spot the signs? *Computer Fraud & Security*. 2007, 3 (2007), 10–15.

[22]   Grazioli, S. 2004. Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet. *Group Decision and Negotiation*. 13, 2 (Mar. 2004), 149–172.

[23]   Halevi, T., Lewis, J. and Memon, N. 2013. A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web - WWW '13 Companion* (New York, New York, USA, 2013), 737–744.

[24]   Herley, C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. *In Proceedings of the 2009 workshop on New*

Security Paradigms Workshop (NSPW '09) (2009), 133–144.

[25]   Hong, K.W., Kelley, C.M., Tembe, R., Murphy-Hill, E. and Mayhorn, C.B. 2013. Keeping Up With The Joneses: Assessing Phishing Susceptibility in an Email Task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 57, 1 (Sep. 2013), 1012–1016.

[26]   Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. 2007. Social phishing. *Communications of the ACM*. 50, (2007), 94–100.

[27]   Koriat, A., Lichtenstein, S. and Fischhoff, B. 1980. Reasons for confidence. *Journal of Experimental Psychology: Human Learning and Memory*. 6, 2 (1980), 107–118.

[28]   Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. 2007. Protecting people from phishing: the design and evaluation of an embedded training email system. *Proceedings of ACM CHI 2007 Conference on Human Factors in Computing Systems*. 1, (2007), 905–914.

[29]   Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*. 10, 2 (May 2010), 1–31.

[30]   Lichtenstein, S. and Fischhoff, B. 1977. Do those who know more also know more about how much they know? *Organizational Behavior and Human Performance*. 20, 2 (Dec. 1977), 159–183.

[31]   McAfee Labs Threat Report August 2014: 2014. *http://www.mcafee.com/uk/security-awareness/articles/mcafee-labs-threats-report-q2-2014.aspx*.

[32]   McNicol, D. 2005. *A Primer of Signal Detection Theory*. Taylor and Francis.

[33]   Modic, D. and Lea, S.E.G. 2011. How Neurotic are Scam Victims, Really? The Big Five and Internet Scams. *In Proceedings of the Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology* (2011).

[34]   Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C. 2014. The design of phishing studies: Challenges for researchers. *Computers and Security*. (2014).

[35]   Pattinson, M., Jerram, C., Parsons, K., McCormac, A. and Butavicius, M. 2012. Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*. 20, (2012), 18–28.

[36]   Riek, M., Bohme, R. and Moore, T. 2016. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*. 13, 2 (Mar. 2016), 261–273.

[37]   RSA Online Fraud Report 2014: 2014. *https://www.rsa.com/de-de/perspectives/resources/2014-cybercrime-roundup*.

[38]   Safe browsing - transparency report - Google: 2013. *https://www.google.com/transparencyreport/safebrowsing/*.

[39]   Sasse, M.A., Brostoff, S. and Weirich, D. 2001. Transforming the "weakest link" — a human/computer interaction approach to usable and effective security. *BT Technology Journal*. 19, 3 (2001), 122–131.

[40]   Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. 2010. Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10* (2010), 373–382.

[41]   Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. 2007. Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07* (New York, New York, USA, 2007), 88.

[42]   Symantec Corporation 2014. Internet Security Threat Report. 19, April (2014), 97.

[43]   Thaler, R.H. and Sunstein, C.R. 2009. *Nudge: Improving decisions about health, wealth, and happiness*. Yale.

[44]   "This message may not have been sent by..." warning: 2016. *https://support.google.com/mail/troubleshooter/2411000?hl=en*.

[45]   Thunderbird's Scam Detection: 2016. *https://support.mozilla.org/en-US/kb/thunderbirds-scam-detection#w_thunderbirds-automatic-scam-filtering*.

[46]   Wang, P.A. 2013. Assessment of Cybersecurity Knowledge and Behavior : An Anti-phishing Scenario. *ICIMP 2013: The Eighth International Conference on Internet Monitoring and Protection*. c (2013), 1–7.

[47]   Wang, Y., Leon, P.G., Acquisti, A., Cranor, L.F., Forget, A., Sadeh, N., Wang, Y., Leon, P.G., Acquisti, A., Cranor, L.F., Forget, A. and Sadeh, N. 2014. A field trial of privacy nudges for facebook. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14* (New York, New York, USA, 2014), 2367–2376.

[48]   Wu, M., Miller, R.C. and Garfinkel, S.L. 2006. Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06* (2006), 601.

[49]   Wu, S.-Y. 2009. *PhishDuck : Capturing User Intention in an Email Client to Combat Phishing*. Carnegie Mellon University.

[50]   Zhang, Y., Egelman, S., Cranor, L. and Hong, J. 2006. Phinding Phish: Evaluating Anti-Phishing Tools. (2006).

[51]   Zhang, Y., Hong, J.I. and Cranor, L.F. 2007. Cantina: a content-based approach to detecting phishing web sites. *Proceedings of the 16th international conference on World Wide Web - WWW '07*. (2007), 639.

A. APPENDIX

A.1 Email Screenshots

The sender saliency nudge emails used for the experiment are presented below. The same set of emails were used for the control condition (without any mark-up), the sender saliency condition (without the percentage mark-up and with added highlights over the key metadata – see Figure 1) and the combined condition (with added highlights over the key metadata – see Figure 1).

Phishing Emails

Below are the six phishing emails, collected from existing messages that were found problematic by our university.

From: PayPal Billing<billing@paypal.email.org>
Sent: 10 December 2014 05:51
To: James Nicholas
Subject: You sent an automatic payment – Thank You

58% of your colleagues received a version of this email

PayPal

You sent an automatic payment.

Hello Member,

You sent an automatic payment to Dedicated Servers. Here are the details:

Amount:	$90.00 USD
For:	Dedicated Servers monthly recurring subscription for $90.00 per year for Dedicated Servers, including 30-days money back guarantee. Cancel any time.

Do you confirm this payment?

If this payment was not made by you please immediately take the following steps:

* Login to your account by clicking on the link below :
* Provide requested information to ensure you are the owner of the account
* Find this transaction in HISTORY and click 'Cancel Transaction'

CANCEL TRANSACTION

Please don't reply to this email. It'll just confuse the computer that sent it and you won't get a response.

PayPal Email ID PP1204

From: eBay<ebay@ebay.co.uk>
Sent: 10 December 2014 04:43
To: James Nicholas
Subject: eBay Reset Your Password

0% of your colleagues received a version of this email

Please note that this is a system generated email; please do not reply to this email because it won't reach us. You can contact Customer Support using the help section from the navbar.

ebay eBay sent this message to James Nicholas
Your registered name is included to show this message originated from eBay. Learn more.

Reset Your Password

Dear James,

Change Password

This email was sent automatically by eBay in response to your request to reset your password. This is done for your protection; only you, the recipient of this email can take the next step in the password recovery process.

To reset your password and access your account, either click on the button or copy and paste the following link (expires in 24 hours) into the address bar of your browser:
https://fyp.ebay.co.uk/ChangePassword?reginput=
87bab6900249ce01e54e5424692232a2e82ad2692d258aae0a66363ac78a
13fbdaf4a1b5bb657c25e71d0c93ffeebc974bea4043676ec037795b1d53
157ab38720fbc9fb4b25225a759024686a819d3c

Thank you,
eBay Trust Team

🛡 Marketplace safety tip

• Keep your eBay account secure. Don't reply to any email that asks for your personal information. Find out more about protecting your account.

Email reference id: [#0ee73a202a924f1eb20467490a34e06a#]

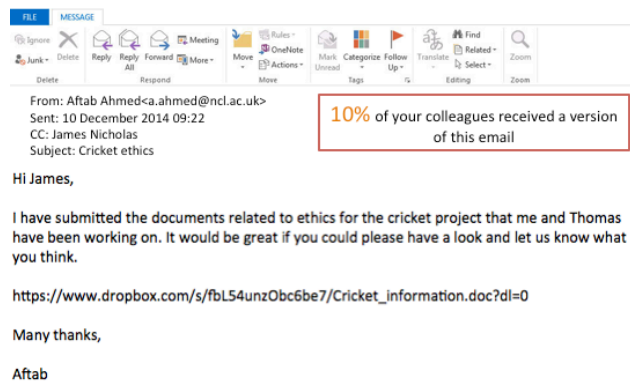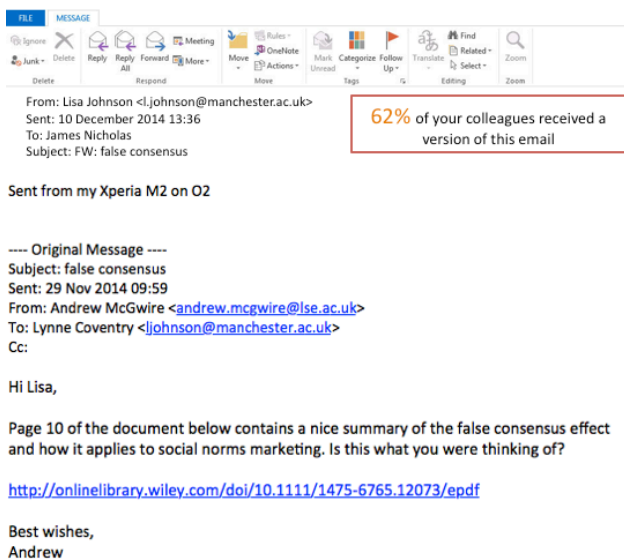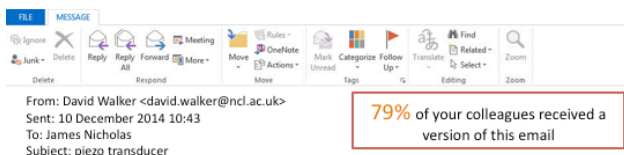Learn More to protect yourself from spoof (fake) emails.

eBay will periodically send you required emails about the site and your transactions. Read our Privacy Policy and User Agreement if you have any questions.

This email was sent by eBay Europe S.à r.l., which may make use of its affiliates to provide the eBay services. If you are a non-EU resident, please find the contact data of your contracting party in the User Agreement.

Copyright © 2014 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. eBay and the eBay logo are trademarks of eBay Inc. eBay Imprint.

Genuine Emails
Below are the twelve genuine emails, collected by the authors.

From: Lisa Johnson <l.johnson@manchester.ac.uk>
Sent: 10 December 2014 13:36
To: James Nicholas
Subject: FW: false consensus

62% of your colleagues received a version of this email

Sent from my Xperia M2 on O2

---- Original Message ----
Subject: false consensus
Sent: 29 Nov 2014 09:59
From: Andrew McGwire <andrew.mcgwire@lse.ac.uk>
To: Lynne Coventry <ljohnson@manchester.ac.uk>
Cc:

Hi Lisa,

Page 10 of the document below contains a nice summary of the false consensus effect and how it applies to social norms marketing. Is this what you were thinking of?

http://onlinelibrary.wiley.com/doi/10.1111/1475-6765.12073/epdf

Best wishes,
Andrew

From: Aftab Ahmed<a.ahmed@ncl.ac.uk>
Sent: 10 December 2014 09:22
CC: James Nicholas
Subject: Cricket ethics

10% of your colleagues received a version of this email

Hi James,

I have submitted the documents related to ethics for the cricket project that me and Thomas have been working on. It would be great if you could please have a look and let us know what you think.

https://www.dropbox.com/s/fbL54unzObc6be7/Cricket_information.doc?dl=0

Many thanks,

Aftab

From: David Walker <david.walker@ncl.ac.uk>
Sent: 10 December 2014 10:43
To: James Nicholas
Subject: piezo transducer

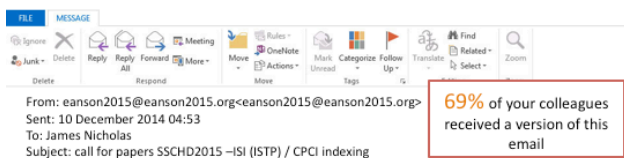79% of your colleagues received a version of this email

Hi - does anyone have a spare large'ish piezo transducer in the bottom of their electronics draw? I need one in a bit of a hurry.

Ideally I'm looking for something 40mm diameter and up - I have a smaller one already. Something like this would be great: http://www.creative-science.org.uk/piezo/piezo1.jpg

Thanks,

Dave

From: eanson2015@eanson2015.org<eanson2015@eanson2015.org>
Sent: 10 December 2014 04:53
To: James Nicholas
Subject: call for papers SSCHD2015 –ISI (ISTP) / CPCI indexing

69% of your colleagues received a version of this email

The 2015 International conference on Social Science and Contemporary Humanity Development

http://www.sschd2015.org/

Dear author

The 2015 International conference on Social Science and Contemporary Humanity Development SSCHD2015 will be held on February 6-8, 2015 in Wuhan, Hubei, China. The SSCHD2015 offers a great opportunity to bring together professors, researchers and scholars around the globe a great platform to deliver the latest innovative research result and the most recent development and trends in Social Science and Humanity Development field.

Publication

SSCHD2015 conference proceedings will be published by DEStech Publications. DEStech will have the CD-ROM indexed in ISTP/CPCI and Google Book Search.

Topics of interest for submission include, but are not limited to:
Sociology and Political Science
Cultural Studies and Humanities
Law and Education
Management and Economics
Social Science and Contemporary Humanity Development
Conference Notices
All submitted papers MUST be written in English.
Any submission must not have been, or will not be published elsewhere or submitted to another conference before the review notification date of this conference.
All submissions will be peer-reviewed based on originality, technical quality and presentation.
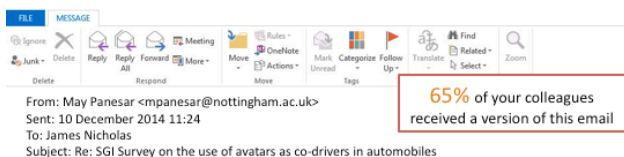Each paper should be at least 3 pages or longer.

Submission
Please submit your paper via easychair: https://easychair.org/conferences/?conf=sschd2015
Please submit your paper Email: SSCHD2015@163.com

Important dates
Paper submission due to: December 5th, 2014

Organizer Contact:
Email: SSCHD2015@163.com(contact SSCHD2015 organizer)
TEL: (+86) 15342340792

From: May Panesar <mpanesar@nottingham.ac.uk>
Sent: 10 December 2014 11:24
To: James Nicholas
Subject: Re: SGI Survey on the use of avatars as co-drivers in automobiles

65% of your colleagues received a version of this email

*Apologies for cross posting*

Dear Member,

One of our Ph.D. students, Tom Matko, is conducting his Ph.D research on the topic of avatar co-driver technologies. If you are of legal driving age with vehicle driving experience, I would like to invite you to participate in this survey, which will support the completion of Tom's Ph.D. thesis.

This survey will help Tom collect people's thoughts on the use of avatars in cars ('avatar co-driver technologies'), and what kind of avatars people would like to see in a car.

If you can spare the time, the survey takes most people less than 20 minutes to complete. To complete the survey, please use the following website link:

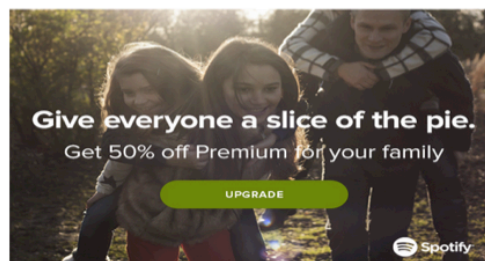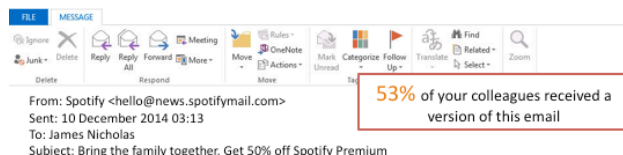https://www.surveymonkey.com/s/MDDR8D8

AVATAR EXAMPLES
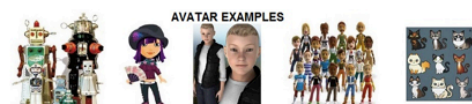
If you have any questions about how to complete the survey, or any other related issues to this topic, please contact the PhD student by e-mail:
tom.matko@btinternet.com.

We would very much appreciate your help with this research project, that contributes to our knowledge in the field of Serious Games.
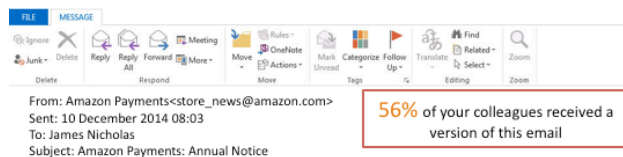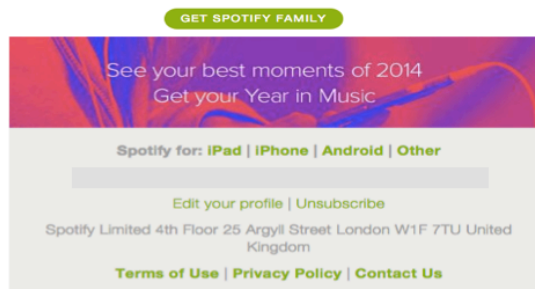
Kind regards,
Pam

From: Spotify <hello@news.spotifymail.com>
Sent: 10 December 2014 03:13
To: James Nicholas
Subject: Bring the family together. Get 50% off Spotify Premium

53% of your colleagues received a version of this email

Spotify

Give everyone a slice of the pie.
Get 50% off Premium for your family

UPGRADE

Happy holidays!

Spotify Family is a great way to share Premium with the people you love.

They get 50% off. You get one simple bill. Everyone gets their own account. No hassle. No tantrums.

GET SPOTIFY FAMILY

See your best moments of 2014
Get your Year in Music

Spotify for: iPad | iPhone | Android | Other

Edit your profile | Unsubscribe

Spotify Limited 4th Floor 25 Argyll Street London W1F 7TU United Kingdom

Terms of Use | Privacy Policy | Contact Us

From: Amazon Payments<store_news@amazon.com>
Sent: 10 December 2014 08:03
To: James Nicholas
Subject: Amazon Payments: Annual Notice

56% of your colleagues received a version of this email

Greetings from Amazon Payments:

Each year we send out a notice to every person who has an active Amazon Payments account. This notice is not a bill; it contains important information about our privacy practices, changes we are making to the availability of certain services, and how you can report errors or unauthorized transactions related to your account.

We appreciate the trust that you have put in Amazon Payments by using our services and want to make sure you are informed about our policies and practices. We know that you care how information about you is used and shared. To help you understand our privacy practices, we have detailed how we collect, use and safeguard your personal and financial information in our Privacy Notice. See Privacy Notice.

Our Unauthorized Transaction Policy describes how you can report to us any billing errors or unauthorized transactions involving the use of your account balance or registered bank account. It also describes our liability and your rights for these types of errors or transactions. See Unauthorized Transaction Policy.

Additionally, we have updated the terms and conditions of our User Agreement that apply to your use of the products and services provided by Amazon Payments. Our updated User Agreement revises certain terms (including, among other things, the elimination of person-to-person payments). Our new User Agreement will become effective on October 13, 2014, which is more than 30 days from when we first posted our updated User Agreement. By continuing to use our services after October 13, 2014, you are agreeing to be bound by the terms and conditions of our new User Agreement. See User Agreement.

Please take a moment to review these changes which may also be found by clicking the User Agreement/Policies link on our web site at https://payments.amazon.com.

If you have questions or concerns about this information, please contact us by signing in to your Amazon Payments account and clicking on the Contact Us link here or by writing to us at Amazon Payments, Attn: Compliance, P.O. Box 81226 Seattle, Washington 98108-1226.

Thank you for using Amazon Payments.

Sincerely,
The Amazon Payments Team

Email 1 (top left):

From: customer.services@eversure.com <customer.services@eversure.com>
Sent: 10 December 2014 14:25
To: James Nicholas
Subject: Your Eversure Cycle Insurance Discount

5% of your colleagues received a version of this email

Eversure INSURANCE

Thank you for visiting Eversure.com.

Your promotion code has been validated and will give you an additional discount when you make your purchase online. Remember our online prices are already discounted by 25%, so there are some great savings to be made!

Your promotion code MONCY10 is valid for 1 year. Click here to return to our website, where your discount code will be applied automatically.

If there are any questions that you have about our insurance then please do not hesitate to contact us and we will be pleased to help.

Your Discount Code

Kind Regards
Eversure Insurance
Bury House, 1-3 Bury Street, Guildford, Surrey GU2 4AW
Tel: 01483 347333 (Our lines are open Monday – Friday 9am-5.30pm, excluding Public Holidays)
We welcome your feedback – complete our short survey and Receive a £10 Wine Voucher!

Eversure Insurance is a trading name of MyFinance.com Limited, a company registered in England and Wales no. 6751893, which is authorised and regulated by the Financial Conduct Authority, register number 501311. You can check this on the Financial Services Register by visiting the FCA's website http://www.fsa.gov.uk/register/home.do or by contacting the FCA on 0800 111 6768.

We are permitted by the FCA to arrange and deal in non-investment insurance contracts. Our registered office address is: MyFinance.com Ltd, Bury House, 1-3 Bury St, Guildford, Surrey, England, GU2 4AW.

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. This message may contain confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately if you have received this e-mail by mistake and delete this e-mail from your system.

Please note that telephone calls may be recorded for monitoring, training and security purposes. WARNING: Although we have taken reasonable precautions to ensure no viruses are present in this email, we cannot accept responsibility for any loss or damage arising from the use of this email or attachments.

Email 2 (bottom left):

From: Jessica Walsh<jessicaw@coventry.ac.uk>
Sent: 10 December 2014 15:29
To: James Nicholas
Subject: FW:

5% of your colleagues received a version of this email

Sorry
http://psycnet.apa.org/journals/ccp/74/6/1017/

---- Original Message ----
Subject:
Sent: 6 Jan 2015 09:59
From: Jessica Walsh <jiwalsh@manchester.ac.uk>
To: Lynne Coventry <jnicholas@mmu.ac.uk>
Cc:

Hi Lynne,

Page 10 of the attached document contains a nice summary of the false consensus effect and how it applies to social norms marketing. Is this what you were thinking of?

Best wishes,
Andrew

Email 3 (top right):

From: Nick Oliver via LinkedIn<invitations@linkedin.com>
Sent: 10 December 2014 15:29
To: James Nicholas
Subject: Nick Oliver's invitation is awaiting your response

3% of your colleagues received a version of this email

Linked in™

Nick Oliver would like to connect on LinkedIn. How would you like to respond?

Nick Oliver
Usability Researcher

Confirm you know Nick

You received an invitation to connect. LinkedIn will use your email address to make suggestions to our members in features like People You May Know. Unsubscribe
If you need assistance or have questions, please contact LinkedIn Customer Service.

Email 4 (bottom right):

From: Nick K<nkutwal07@gmail.com>
Sent: 10 December 2014 08:09
To: James Nicholas
Subject: Risk of other cancers in familial pancreatic cancer

0% of your colleagues received a version of this email

Dear Dr. James Nicholas

My name is Nikhil Kaur. I am a sophomore currently attending Hillark High School, where I am enrolled in the Science Research Program. This program is one that has been designed to allow students the opportunity to conduct individual research projects involving the participation of a mentor at a research facility. While enrolled in this program, I have chosen an area of science that I have a strong interest in: Orthopedic research. Additionally I have a strong interest in joints and bones. After the successful completion of such projects in Stony Brook University, I have a strong intention in entering into various science competitions such as Intel, Siemens Competition, The Long Island Science and Engineering Fair, and other competitions as well. In recent journal article searches, I discovered your publications involving *"Risk of other cancers in familial pancreatic cancer"*, however, I have been unable to access it.

Would you be king enough to forward me any of your recent publications relating to these applications? Additionally, would you have an interest in mentoring a motivated student, such as myself, to conduct similar research during the summer? Any assistance or guidance that you would be able to lend in this matter would be greatly appreciated. I please find a copy of my resume for your review below, and I greatly look forward to hearing from you.
www.nikk.net/resume(5).doc

Thank you, in advance, for your time and efforts in this matter

Sincerely, Nikhil Kaur