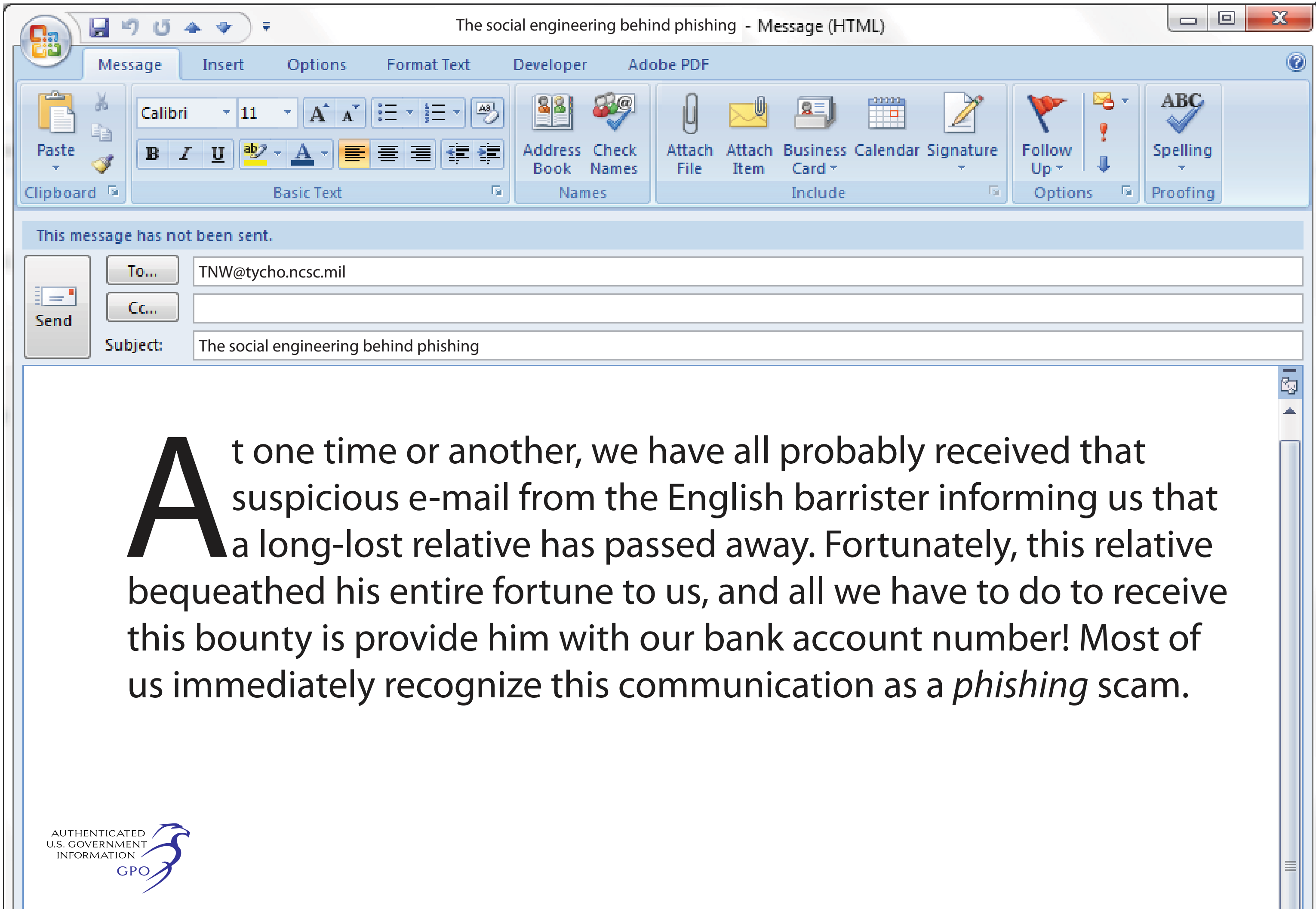
The social engineering behind phishing

Christopher B. Mayhorn
Emerson Murphy-Hill
Olga A. Zielinska
Allaire K. Welk



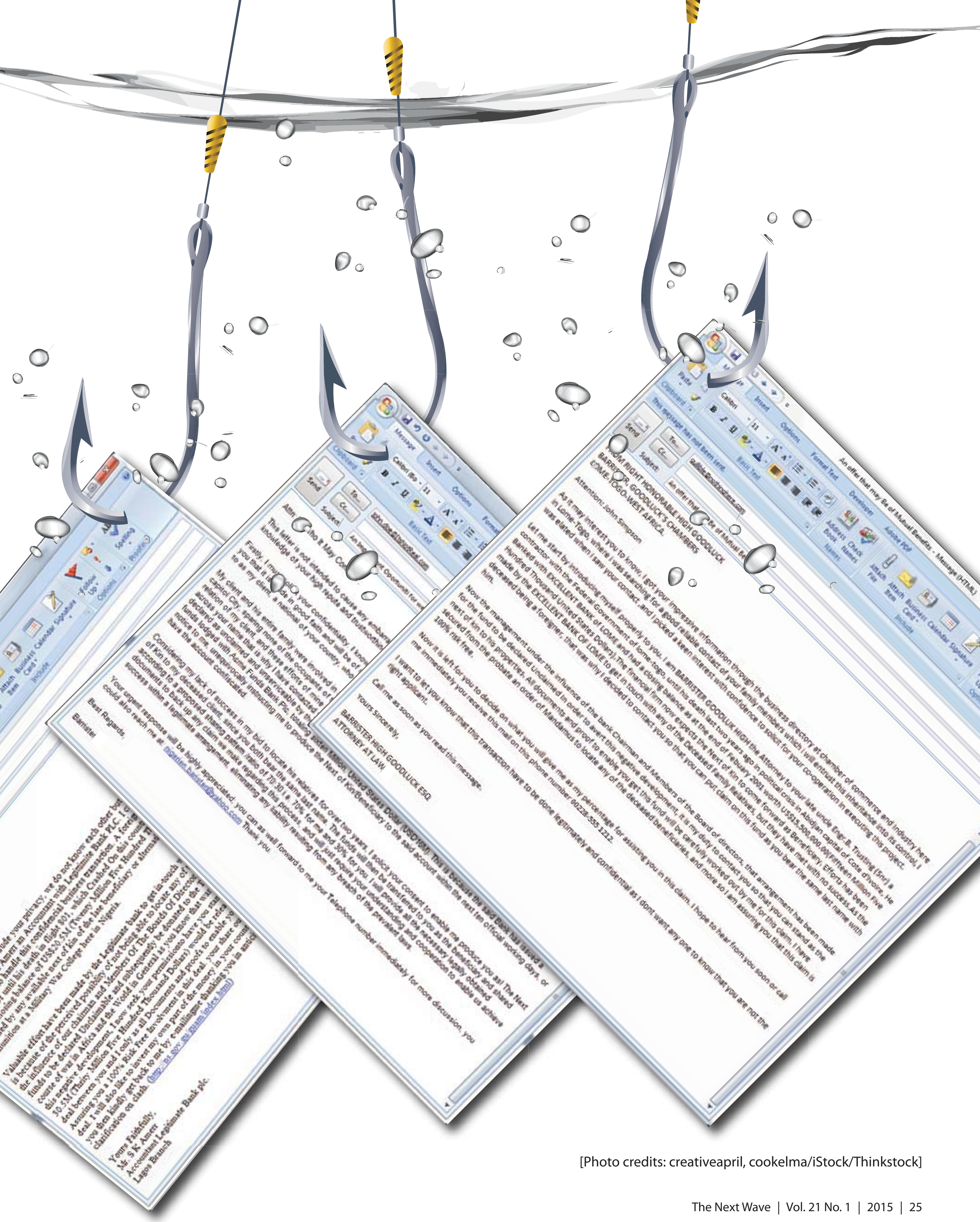
This message has not been sent.

To... TNW@tycho.ncsc.mil

Cc...

Subject: The social engineering behind phishing

At one time or another, we have all probably received that suspicious e-mail from the English barrister informing us that a long-lost relative has passed away. Fortunately, this relative bequeathed his entire fortune to us, and all we have to do to receive this bounty is provide him with our bank account number! Most of us immediately recognize this communication as a *phishing* scam.



[Photo credits: creativeapril, cookelma/iStock/Thinkstock]

Defining the phishing problem

Phishing is a social engineering tactic that cybercriminals use to trick people into revealing sensitive personal information, such as their date of birth, banking details, credit card information, or social security number. This is known as a *semantic* (i.e., language-based) attack because the criminals have targeted the computer user rather than technical aspects of the system. Users are typically sent an e-mail that appears to be from a known entity such as an established organization or individual that requires the user to reconfirm personal information by entering it via a supplied link within the text of the e-mail. These e-mails usually include "authentic" graphics and images that trick individual users into believing that the communication and request for information is legitimate.

If all attacks were so obvious, most people would have little trouble avoiding an adverse outcome. While communications ostensibly from Nigerian princes and former Iraqi generals are always suspect, criminal activities are becoming increasingly more frequent and difficult to detect. For instance, Kaspersky Lab reported that there were as many as 37.3 million attacks in 2013, up from 19.9 million in 2012 [1]. Given the sheer number of attacks, it is likely that a percentage will be successful. After all, criminals would not engage in this activity if some individuals did not provide the requested information. For the phishing victim, personal costs associated with falling prey to such an attack can include loss of time, increased stress, monetary losses, and damaged credit. Some estimates indicate that each individual phishing attack costs approximately $866, and phishing attacks overall contribute to over $3 billion in annual financial losses [2].

These direct costs of phishing to individuals are joined by other direct costs such as those incurred by private sector financial institutions as they attempt to shore up compromised systems and fix damaged credit. Likewise, less direct costs might be incurred by legitimate business entities that lose profits as users become more hesitant to trust online access. Costs continue to grow as government assets are deployed for investigation and enforcement purposes.

Faced with these disheartening statistics along with a steadily increasing price tag, what can be done to prevent people from being victimized? Previous efforts to combat the phishing problem have focused on building technological solutions, such as phishing web-page detectors, yet some authors (e.g.,[3]) have suggested that regardless of how security-related technology is improved, successful solutions must address the "people problem." The purpose of this article is to describe and summarize our NSA-funded research program at North Carolina State University (NCSU) that attempts to address this topic.

The NCSU Science of Security Lablet, one of only four in the United States funded by the NSA, has begun to investigate phishing using a multidisciplinary approach. Team members come from diverse backgrounds, including the university's departments of psychology and computer science.

Below, we describe a series of studies that sought to answer broad questions regarding who is at risk, what factors predict phishing susceptibility, and how phishing susceptibility might be reduced through the implementation of training programs. Lastly, we conclude with a section that describes how our findings might inform the design of future tools that implement tailored warning systems.

Who is at risk?

To better understand who is at risk when confronted with a phishing e-mail, we conducted an initial survey that asked 155 respondents to describe their previous experiences with phishing attempts and the related consequences [4]. Virtually **all** participants indicated that they had received a phishing e-mail at some time in the past, and 22% reported that these attempts were successful. In addition, 84% of participants readily identified e-mail as the media where they were most likely to encounter phishing messages, but participants also described other instances where phishing messages were delivered via instant messaging, job boards, or social networking sites. As the following response indicates, phishers are becoming very creative in their efforts:

> I applied for a part time job through Craigslist and had to do a credit check to successfully apply. I thought it was OK since lots of employers now do credit checks. I entered my social and lots of other information. . . . By next week I had several pings in my credit report of suspicious activity. Someone had taken out a credit card in my name and also tried to get

> a loan. I was scared, honestly, that someone could use my information in that way. I was also angry . . .

When asked about the content of phishing messages, qualitative comments from respondents suggested that phishing communications often sound “too good to be true” and include “exciting or unbelievable offers.” In addition, comments also revealed phishing attacks often use a “strong pitch,” and attempt to elicit “a feeling of urgency to get stuff done now,” by using “a limited time offer or high-pressure tactics” in an attempt to get victims to act quickly.

Although we believed the costs of getting phished were obvious, these results are informative because they indicate that the effects are not limited to financial costs or loss of material items only (e.g., money, property, etc.), but may have social ramifications as well (e.g., loss of trust, embarrassment). Qualitative comments underscored potential psychological impacts resulting from phishing attacks; participants referenced negative emotions, such as “embarrassment, shame or loss of self-confidence.”

What makes someone susceptible to phishing attacks?

Because we are all apparently at risk when it comes to phishing attempts, our next efforts were to clarify why users might be at risk. Previous research indicated that cognitive factors, such as attentional vigilance to cues in the computing environment, serve as a key component in avoiding phishing [5, 6]. Other studies have identified how users who fall prey to phishing tend to haphazardly rely on perceptual cues, such as the layout of a webpage, or on social cues, such as whether or not the sender of an e-mail is known [7]. In effect, users try to ascertain the veracity of cues to determine whether they can trust the sender prior to making a security-related decision. This is problematic because criminals often manipulate aspects of digital communications that cultivate trust, thereby increasing phishing susceptibility [8].

As people tend to vary with regard to individual differences in cognition, perception, and dispositional factors, we sought to determine what factors make some users more susceptible to phishing than others [9]. In this particular study, 53 undergraduate students completed a battery of cognitive tests and a survey designed to assess impulsivity, trust, and personality traits before they performed an e-mail categorization task that required them to discriminate legitimate e-mails from phishing attempts.

Our results indicated that individuals who possessed personality characteristics such as reserved behavior consistent with introverts, low impulsivity, and decreased trust were more likely than others to accurately identify phishing messages. Likewise, previous experience such as suffering a monetary loss also decreased susceptibility to phishing attacks. These findings taken together suggest that some people are more susceptible to phishing attacks than others, so efforts to ameliorate phishing might work best if efforts are focused on those most at risk (i.e., those who are extroverted, impulsive, and trusting).

Because these are measurable characteristics and there are a variety of psychological instruments available to assess these behavioral constructs, it is feasible that a quantifiable profile of phishing susceptibility could be constructed. While promising, such efforts would need to be validated empirically and psychometrically.

Although the previous work suggests that individual differences are important determinants of phishing susceptibility, human behavior does not occur in a vacuum. One caveat that has pervaded social science research for the last 150 years is that behavior varies by social context. Given increasing workplace diversity and the globalization of the business industry coupled with enhanced communication enabled by technology, interaction with geographically distributed multinational teams is now commonplace to most of us.

Extending the concept of individual differences to group differences begs the question of whether culture plays a role in phishing susceptibility. To answer this question, we examined self-reported rates of phishing susceptibility and online privacy behaviors from Chinese, Indian, and American samples [10]. We surveyed 164 participants from the United States, India, and China to assess past phishing experiences and the likelihood of engaging in online safety practices (e.g., reading a privacy policy). Results indicated that all nationalities were equally likely to experience phishing attempts yet the prevalence of being successfully phished varied by nationality such that only 9% of Chinese, 14% of Americans, and 31% of Indians had been successfully phished. Thus, Chinese and American respondents were about as likely to get phished yet both of these nationalities were less susceptible than Indian respondents.

We discussed these potential cultural differences in terms of power distance—where low power distance countries, such as the United States, could be considered individualistic and more challenging of authority than high power distance countries, like India, that tend to convey high levels of respect to authorities where compliance with information requests might be more likely.

With regard to taking protective action to prevent information loss, cultural differences were also observed such that Chinese and Americans were more likely than Indian respondents to report destroying old documents, yet Americans were more likely than either Chinese or Indians to actively search a web page for the secure padlock icon when making online transactions. These results suggest that cultural background might be another factor to consider when developing a profile of phishing susceptibility. Such a profile would theoretically be useful in identifying those most in need of security training.

Can training prevent phishing?

Antiphishing training is one approach to making the user aware of phishing thereby acting as a barrier to attacks [11]. In the past, antiphishing training has ranged from a list of Internet user tips to a cartoon that helps explain user tips in a story format to even a game that provides embedded training against phishing [12]. From past research, training efforts were more effective when shown in a real-world context [13]. Additionally, another study revealed that the level of threat perception determines the quality of protective action taken because perception of a high level of threat motivated participants to act and change their behavior. Likewise, such threat manipulations also increased the retention of information [14].

Given these general considerations regarding the development of an antiphishing training program, we developed two experimental antiphishing training conditions: one that conveyed real-world consequences to trainees, and one that attempted to induce perceptions of high threat [15]. The training on real-world consequences was delivered via three videos that reported on different news stories where identity theft occurred as a result of phishing, followed by an emotional interview with a victim of a fake money order scam. The second training condition used three news articles selected with the intention of raising the level of threat perceived by participants. These articles included recent news stories about how Facebook is collecting data and selling it along with news stories regarding the recent leak at NSA perpetrated by an insider. These two experimental antiphishing training conditions were compared to a third control condition that showed participants a cooking video.

Ninety-six participants completed a baseline e-mail categorization task in which they had to discriminate legitimate e-mails from phishing attempts before being randomly assigned to one of the three training conditions. After training was completed, a second e-mail categorization task was completed. An increased rate of accurately identifying phishing e-mails on the second task compared to the baseline was observed in all training conditions—suggesting that training was generally effective. Unfortunately, there were no statistically significant differences between the experimental training conditions and the control condition; although, trends suggested that heightening the threat perception slightly enhanced participants' abilities to detect phishing messages.

While these particular training manipulations did not produce compelling results, another approach would be to train individuals less experienced with computer security on how experts conceptualize phishing attacks. In essence, such training would allow novices to learn from more experienced experts.

How novices and experts conceptualize attacks

One method to quantify differences in experience includes examining differences between the mental models of security novices and experts. Mental models are internal representations that users develop of a concept or system. Mental models grow as individuals interact with a system or concept; eventually, the user will be able to use his or her developed mental models to predict or explain the system or concept [16]. Accordingly, as users develop expertise, they have qualitative changes in their mental models. Experts are able to quickly analyze a situation or case and make quick decisions because of their coherent organization of information. Thus, an underlying tenet of naturalistic decision-making research [17] suggests that training novices to use expert-level tactics might be useful in reducing errors (in this case, reducing phishing susceptibility).

Our most recent phishing-related project assessed how the mental models of computer security novices varied from those of computer security experts [18]. Twenty-eight participants (20 novices and 8 experts) were asked to rate the strength of the relationship among pairs of phishing-related concepts. These relatedness ratings were entered into Pathfinder, a statistical software tool that represents pairwise proximities in a network [19]. Preliminary findings suggest that novices and experts had significantly different mental models with regard to the prevention of phishing attacks and the trends and characteristics of attacks.

Expert mental models were more complex with more links between concepts, and this could have implications for training. For example, the aggregate expert model illustrated "unknown sender" as a central node connected to "social engineering," "legitimate appearance," "link," "attachment," and "bad spelling/grammar"; whereas, novices only linked "unknown senders" to "attachment" and "link." This illustrates that experts likely have a more comprehensive understanding of how unknown senders can relate to a broad array of phishing trends and characteristics. Training programs might aim to replicate this expert model in novices by providing information regarding the interconnectedness of these trends and characteristics related to unknown senders.

Future directions

While efforts to promote cybersecurity through training might yet prove to be an effective means to reducing phishing susceptibility, it is unclear whether users will be motivated to spend the time and energy to attend such sessions. Also, it is unrealistic to presume that people will be constantly on guard to protect themselves from potential online security threats, so perhaps this function should be allocated to the technology involved. It is likely that such a technology would include some type of warning functionality that would serve to alert users when their information is at risk. To address the potential characteristics of such a system, there are a number of theoretical frameworks within the hazard communication literature that have been used to describe response to warning messages where some action has to be taken when a threat is detected [20, 21, 22].

In all of these theoretical models, members of the public encounter a warning message that describes the nature of a hazard and suggests courses of action to avoid the consequences. Ultimately, the individual decision maker must act to either comply with or ignore the warning message. A growing realization within the hazard communication literature is that effective warning messages must be tailored to match the hazardousness of the situation or to the user's characteristics to benefit comprehension [23]. Our initial efforts described above provide data to build a profile of at-risk users who are especially susceptible to phishing thereby providing the knowledge necessary to tailor effective warning messages. For instance, foreknowledge of a user's impulsive nature from previous online activities might suggest that the inclusion of an "Are you sure?" dialog box following an initial attempt to follow a suspicious link might result in temporal delay that allows a more thoughtful response. However, this example also illustrates that the development of such a tool must include a consideration of usability and technology adoption to ensure that potential solutions are acceptable to users [24].

Conclusions

Given the potential costs to individuals, organizations, and governments, phishing is a cybersecurity problem that demands attention in terms of both research and practice. As the results described above indicate, we are starting to answer some important questions that can be useful in designing countermeasures to reduce the likelihood of data loss. By understanding how individual differences in cognition, perception, and behavior predict phishing susceptibility, we can identify and target vulnerability for training interventions. We have already investigated whether or not specific training tactics help to reduce phishing susceptibility, but much more work needs to be done.

Lastly, we have begun to compile a set of functional requirements to guide development of future technological tools that help to protect our information in cyberspace.

About the authors

Christopher B. Mayhorn is a professor and the program coordinator of the Human Factors and Applied Cognition Psychology Program at North Carolina State University (NCSU). He earned a BA from The Citadel in 1992, an MS in 1995, a Graduate Certificate in Gerontology in 1995, and a PhD in 1999 from the University of Georgia. He also completed a postdoctoral fellowship at the Georgia Institute of Technology. Dr. Mayhorn's current research interests include everyday memory, decision making, human-computer interaction, and safety and risk communication. Dr. Mayhorn has more than 50 peer-reviewed publications to his credit, and his research has been funded by government agencies such as the National Science Foundation and the NSA. Currently, he serves as the chair of the Technical Program Committee for the Annual Meeting of the Human Factors and Ergonomics Society and is on the editorial board of *Human Factors*. He was also recently named one of eighteen University Faculty Scholars at NCSU.

Emerson Murphy-Hill is an assistant professor in computer science at NCSU. He earned a BS from The Evergreen State College in 2004 and a PhD from Portland State University in 2009. He also completed a postdoctoral fellowship at the University of British Columbia in 2010. He directs the Developer Liberation Front, a research group dedicated to exploring the intersections of human-computer interaction and software engineering.

Olga A. Zielinska is a PhD student in the Human Factors and Applied Cognition Psychology Program at NCSU. She recently earned her MS degree from NCSU; her thesis focused on how the formatting of search results can affect how Internet users search for health information. She has a BS in biomedical engineering from Drexel University.

Allaire K. Welk is a PhD student in the Human Factors and Applied Cognition Psychology program at NCSU. She recently earned her MS degree from NCSU; her thesis focused on the phenomenon of inattentional blindness as it relates to informational displays. She has a BA in psychology from NCSU.

References

[1] Kaspersky Lab. "37.3 Million Users Experienced Phishing Attacks in the Last Year" [Press Release]. 20 Jun 2013. Available at: http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year.

[2] Gartner. "Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks" [Press release]. 17 Dec 2007. Available at: http://www.gartner.com/it/page.jsp?id=565125.

[3] Schneier B. *Secrets and Lies: Digital Security in a Networked World.* New York (NY): Wiley & Sons; 2000. ISBN-13: 978-0-471-45380-2.

[4] Kelley CM, Hong KW, Mayhorn CB, Murphy-Hill E. "Something smells phishy: Exploring definitions, consequences, and reactions to phishing." In: *Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting;* 2012. doi: 10.1177/1071181312561447.

[5] Downs JS, Holbrook MB, Cranor LF. "Decision strategies and susceptibility to phishing." In: *Proceedings of the Second Symposium on Usable Privacy and Security;* 2006. doi: 10.1145/1143120.1143131.

[6] Vishwanath A, Herath T, Chen R, Wang J, Rao HR. "Why do people get phished? Testing individual differences in phishing vulnerability with an integrated, information processing model." *Decision Support Systems.* 2011;51(3):576–586. doi: 10.1016/j.dss.2011.03.002.

[7] Jagatic TN, Johnson NA, Jakobsson M, Menczer F. "Social phishing." *Communications of the ACM.* 2007;50(10):94–100. doi: 10.1145/1290958.1290968.

[8] Workman M. "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security." *Journal of the American Society for Information Science and Technology.* 2008;59(4):662–674. doi: 10.1002/asi.v59:4.

[9] Mayhorn CB, Welk AK, Zielinska OA, Murphy-Hill E. "Assessing individual differences in a phishing detection task." In: *Proceedings of the 19th World Congress of the International Ergonomics Association.* Melbourne, Australia. (In press).

[10] Tembe R, Zielinska O, Liu Y, Hong KW, Murphy-Hill E, Mayhorn CB, Ge X. "Phishing in international waters: Exploring cross-cultural differences in phishing conceptualizations between Chinese, Indian, and American samples." In: *Proceedings of HotSoS: Symposium and Bootcamp on the Science of Security;* 2014. doi: 10.1145/2600176.2600178.

[11] Mayhorn CB, Nyeste PG. "Training users to counteract phishing." *Work.* 2012;41(Suppl 1):3549–3552. doi: 10.3233/WOR-2012-1054-3549.

[12] Alnajim A, Munro M. "An anti-phishing approach that uses training intervention for phishing websites detection." In: *Sixth International Conference on Information Technology: New Generations, 2009. ITNG '09;* 2009. doi: 10.1109/ITNG.2009.109.

[13] Kumaraguru P, Sheng S, Acquist A, Cranor L, Hong J. "Lessons learned from a real-world evaluation of anti-phishing training." In: *eCrime Researchers Summit;* 2008. doi: 10.1109/ECRIME.2008.4696970.

[14] Davinson N, Sillence E. "It won't happen to me: Promoting secure behaviour among internet users." *Computers in Human Behavior.* 2010;26(6):1739–1747. doi: 10.1016/j.chb.2010.06.023.

[15] Zielinska OA, Tembe R, Hong KW, Xe G, Murphy-Hill E, Mayhorn CB. "One phish, two phish, how to avoid the Internet phish: Analysis of training strategies to detect phishing e-mails." In: *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting;* 2014. doi: 10.1177/1541931214581306.

[16] Norman DA. "Some observations on mental models." In: Genter D, Stevens AL, editors. *Mental Models.* Hillsdale (NJ): Erlbaum; 1983. p. 7–14.

[17] Klein G. *Sources of Power.* Cambridge (MA): MIT Press; 1999. ISBN-13: 978-0262112277.

[18] Zielinska OA, Welk AK, Murphy-Hill E, Mayhorn CB. (in press). "Exploring expert and novice mental models of phishing." In: *Proceedings of HotSoS: Symposium and Bootcamp on the Science of Security;* 2015. doi: 10.1145/2746194.2746216.

[19] Rowe AL, Cooke NJ. "Measuring mental models: Choosing the right tools for the job." *Human Resource Development Quarterly.* 1995;6(3):243–255. doi: 10.1002/hrdq.3920060303.

[20] Lindell MK, Perry RW. (2004). *Communicating Environmental Risk in Multiethnic Communities.* Thousand Oaks (CA): Sage Publications; 2004. ISBN: 0-7619-0650-9.

[21] Rogers WA, Lamson N, Rousseau GK. "Warning research: An integrative perspective." *Human Factors,* 2000;42(1):102–139. doi: 10.1518/001872000779656624.

[22] Wogalter MS, Dejoy, DM, Laughery, KR. *Warnings and risk communication.* London: Taylor and Francis; 1999. ISBN: 0748402667.

[23] Wogalter MS, Mayhorn CB. "Providing cognitive support with technology-based warning systems." *Ergonomics,* 2005;*48*(5):522–533. doi: 10.1080/00140130400029258.

[24] Venkatesh V, Davis F D. "A theoretical extension of the technology acceptance model: Four longitudinal field studies." *Management Science.* 2000;46(2):186–204. doi: 10.1287/mnsc.46.2.186.11926.