Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content

TIAN LIN, DANIEL E. CAPECCI, DONOVAN M. ELLIS, HAROLD A. ROCHA, SANDEEP DOMMARAJU, DANIELA S. OLIVEIRA, and NATALIE C. EBNER, University of Florida

Phishing is fundamental to cyber attacks. This research determined the effect of Internet user age and email content such as weapons of influence (persuasive techniques that attackers can use to lure individuals to fall for an attack) and life domains (a specific topic or aspect of an individual's life that attackers can focus an email on) on spear-phishing (targeted phishing) susceptibility. In total, 100 young and 58 older users received, without their knowledge, daily simulated phishing emails over 21 days. A browser plugin recorded their clicking on links in the emails as an indicator of their susceptibility. Forty-three percent of users fell for the simulated phishing emails, with older women showing the highest susceptibility. While susceptibility in young users declined across the study, susceptibility in older users remained stable. The relative effectiveness of the attacks differed by weapons of influence and life domains with age-group variability. In addition, older compared to young users reported lower susceptibility awareness. These findings support effects of Internet user demographics and email content on susceptibility to phishing and emphasize the need for personalization of the next generation of security solutions.

CCS Concepts: • **Security and privacy → Phishing**; **Social aspects of security and privacy**; • **Human-centered computing → Empirical studies in HCI**; • **Social and professional topics → Seniors**;

Additional Key Words and Phrases: Phishing, Emails, Susceptibility, Aging, Weapons of Influence, Life Domains

ACM Reference format:
Tian Lin, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira, and Natalie C. Ebner. 2019. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Trans. Comput.-Hum. Interact.* 26, 5, Article 32 (July 2019), 28 pages.
https://doi.org/10.1145/3336141

This research was supported by NSF grant SBE-1450624 and NIH/NIA grant R01 AG057764.
Authors' addresses: T. Lin, D. M. Ellis, H. A. Rocha, and N. C. Ebner, Department of Psychology, University of Florida, 945 Center Drive, Gainseville, FL, USA 32611; emails: {lintian0527, hrocha1, natalie.ebner}@ufl.edu, dellis22@student.gsu.edu; D. E. Capecci and D. S. Oliveira, Department of Electrical and Computer Engineering, University of Florida, 968 Center Drive, Gainesville, FL, USA 32611; emails: dcapecci@ufl.edu, daniela@ece.ufl.edu; S. Dommaraju, Department of Computer and Information Science and Engineering, University of Florida, E301 CSE Building, Gainesville, FL, USA 32611; email: sandeepdommaraju@gmail.com.

1073-0516/2019/07-ART32 $15.00
https://doi.org/10.1145/3336141

1 INTRODUCTION

Phishing emails are a type of targeted email attack where social engineers lure the recipient into performing specific actions such as clicking on a malicious link, opening a malicious attachment, or visiting a web page and entering their personal information (APWG 2014; Hong 2012). These attacks are appealing, not only because they are simple and low cost, but also because they make attack attribution difficult (Bradley 2011; Carr 2011). As a result, phishing is a fundamental component of many cyber attacks and is often used as a first step in advanced persistent threats (APTs; James 2005; Singer and Friedman 2014). Susceptibility to phishing, including spear-phishing (a more targeted variation of phishing, where usually the victim is addressed by name[1]), in older adults is a critical and growing public health concern but is currently largely overlooked in the scientific literature. There are several factors that may make older adults a particular target for such attacks as follows: (i) Older adults are the fastest growing segment of the U.S. population, in part due to the "baby-boomer" generation (National Center for Chronic Disease Prevention and Health Promotion, 2009; United States 2010 Census, 2010); (ii) Older adults often have accumulated financial assets over a lifetime, which they increasingly manage online (Perrin and Duggan 2015); (iii) Many older adults occupy powerful positions in finances and politics and are confronted with a variety of decision-making situations in cyberspace (e.g., clicking on a link in an email and visiting web sites); (iv) Finally, general cognitive-processing capacities and sensitivity to deception decline with age, while self-reported trust increases (Johnson 1990; Mata et al. 2011; Mather 2006; Tentori et al. 2001; Verhaeghen and Salthouse 1997).

Some previous survey-based studies showed that older adults were not more likely to fall for fraud than young adults (Lichtenberg et al. 2016; Ross et al. 2014; Sugiura 2013; Wood et al. 2015). However, these findings referred to more general forms of fraud (e.g., "*Have you been the victim of financial fraud in the past five years (Yes, No)?*"). As Ross et al. (2014) suggested, lack of age effects in susceptibility across some types of fraud does not mean that there are no age-related differences in any type of fraud (e.g., phishing). Also, compared to survey-based studies that largely depend on self-reflection about past experience with fraud, a field experiment can directly capture behavioral response to attempted fraud. Thus, we propose that a behavior-based methodology is particularly advantageous when determining susceptibility to phishing "in the wild" as well as among older adults, considering self-report response biases among older adults (e.g., positivity bias in autobiographical memory; Fernandes et al. 2008; Tomaszczyk and Fernandes 2012).

In addition to Internet user characteristics such as their age as potential risk factors to phishing susceptibility, the specific content of a phishing email may contribute to the effectiveness of the attack, also in interaction with user demographics. The literature suggests a variety of techniques that can be applied to lure users into clicking on malicious email links or procuring personal information. In particular, Cialdini (2007) and Hadnagy (2010) proposed seven psychological principles or weapons of influence that can be applied in phishing emails to lure individuals to fall for the attack. For example, to make the opportunities mentioned in an email seem more valuable, attackers will make those opportunities seem rare (scarcity). In the present study, we used the term "weapons of influence," instead of "principles of influence" from Cialdini (2007), to particularly reflect the malicious intention of attackers who use those strategies in phishing.

In addition to weapons of influence, attackers can focus an email on a specific topic or aspect of an individual's life (life domain; Baltes 1987), which may be particularly relevant to the recipient.

[1]To facilitate reading and connection with the literature, in this paper we do not differentiate between spear-phishing and phishing and use the term 'phishing' in the remainder of the paper.

For example, they can create an email as an advertisement for some medication (health), which potentially appeals to certain demographics (e.g., older adults).

Based on the considerations above and to fill a significant research gap, we conducted a field experiment (user study) over a period of 21 days to investigate susceptibility to phishing (i.e., whether individuals clicked on links in phishing emails) and susceptibility awareness (i.e., individuals' self-reported likelihood of clicking on links in phishing emails) among young and older Internet users. In addition, we examined the extent to which young and older Internet users' susceptibility and susceptibility awareness to phishing emails varied by email content (weapons of influence and life domains).

The study protocol was approved by the Institutional Review Board (IRB) at the University of Florida. The study took place at the participants' homes. During the study interval, 100 young and 58 older Internet users received, without their knowledge, simulated phishing emails from our study team. These emails systematically varied weapons of influence and life domains and contained a web link (URL), which led participants to an accompanying web façade created by our group. A browser plug-in developed for this study recorded all web sites visited by the user during the study. The plug-in also tracked whether users clicked on the embedded links in the simulated phishing emails, which was our central dependent variable and indicated participants' *susceptibility to the phishing emails*. On the last study day, users reviewed 21 previously unseen simulated phishing emails and indicated how likely they would click on the link in each email. This measure served as the indicator of participants' *susceptibility awareness to the phishing emails*.

We found that older women were particularly susceptible to phishing. In addition, young users' susceptibility decreased across the course of the intervention, while older users' susceptibility did not decrease. The effectiveness of phishing emails varied depending on the weapons of influence and life domains. In particular, susceptibility was highest for scarcity and legal emails and lowest for social proof and financial emails. Further, the relative effectiveness of specific weapons of influence differed between young and older users. While young compared to older users showed greater susceptibility to scarcity and authority emails, older compared to young users showed greater susceptibility to reciprocation and liking emails. Older users showed lower susceptibility awareness than young users. In addition, susceptibility awareness varied by the weapons of influence and life domains. In particular, susceptibility awareness was highest for scarcity and legal emails and lowest for social proof and health emails.

Currently, the literature on deception and aging is scarce, especially in the context of cybersecurity. The majority of current research on decision-making in aging focuses on financial or health decisions and is conducted in laboratory settings or via surveys (Peters 2006; Samanez-Larkin and Knutson 2015; Westerman and Davies 2000). Further, current human factors of phishing research has largely focused on general education and anti-phishing training (Caputo et al. 2014), but not on the identification of particularly vulnerable groups among diverse demographics for designing more tailored intervention approaches (for an exception see Neupane et al. 2018). To our knowledge, this study is the first behavioral measurement of aging effects on deception related to phishing emails in an ecologically valid context.

This article starts with a review of related work on phishing as well as on age-related changes in trust and susceptibility to deception. We then provide the theoretical background for the key constructs of weapons of influence and life domains. The literature review concludes with a summary of our central research hypotheses. Next, the article outlines our study methodology and framework, including details about the Phishing Internet Task (PHIT), developed to assess susceptibility to phishing emails. We then report detailed results, before presenting concluding remarks.

2 RELATED WORK

2.1 Phishing

Phishing is a type of cyber social engineering attack, through which adversaries lure the recipient into clicking on a malicious link, opening a malicious attachment, or visiting a web page, procuring the user's personal information. The security of individual Internet users and organizations, all the way up to nation-states, can be affected by such attacks. These attacks constitute a widespread threat; they are increasingly combined with malware and used as gateways for future attacks, such as APTs (James 2005; Fisher 2011; Singer and Friedman 2014; Wrightson 2014). Phishing can leverage emails, instant messaging, social media, and even Quick Response (QR) codes; called QRishing (Vidas et al. 2013). QRishing encourages mobile users to scan unauthenticated QR codes from various places, which directs users to visit malicious websites or install malware. Current protection methods propose the filtering of malicious emails before users see them (usually via machine learning methods) or support decision-making by training users in recognition of suspicious emails (Fette et al. 2007; Sheng et al. 2009; Netcraft Toolbar 2010; Zhang et al. 2007). For example, *Anti-phishing Phil*, which teaches an organization's employees good habits to avoid phishing via a game, is one example of such an effort (Sheng et al. 2007). *PhishGuru* was developed as an embedded training system for identifying phishing in emails (Kumaraguru et al. 2009). Phishing training faces many challenges, not the least of which is that people tend to forget the learned material and fall for the similar malicious emails again a short time after the training (as early as a few weeks). For example, an investigation into the efficacy of anti-phishing exercises in the context of a large organization found that the training had no significant effect on the likelihood that users would click on phishing email links (Caputo et al. 2014). Instead, users typically either clicked on all links or clicked on none, independent of the training.

These previous intervention studies suggest a considerable inter-individual difference in susceptibility to phishing. Some empirical work investigated demographic characteristics of individuals with high susceptibility to phishing and found that women compared to men were more susceptible (Halevi et al. 2015; Sheng et al. 2010). In addition, individuals with a higher capability of deliberative processing, a decision-making process based on reflective reasoning rather than intuitive thinking (Evans 2008, 2010), showed better performance in the differentiation of phishing emails from legitimate emails (Jones et al. 2019). Survey-based studies examined the susceptibility to phishing as a function of personality traits and found that users with higher conscientiousness showed higher likelihood for falling for phishing (Halevi et al. 2015). Some studies also examined susceptibility to phishing as a function of age and found that users between the ages of 18 and 25 years were more susceptible to phishing than other age groups (Kumaraguru et al. 2009; Sheng et al. 2010). These studies considered individuals up to middle age, but not older users (60 years and older). There is some indication that a "golden age" of decision-making occurs in adults aged around 55 years old, which is characterized by high levels of fluid intelligence (e.g., processing speed, working memory) and crystallized intelligence (e.g., experience; Agarwal et al. 2009; Samanez-Larkin 2013). Thus, the middle-aged group may not be particularly at risk for such attacks. However, as we will discuss in more detail below, older users may be particularly vulnerable to phishing but have been under-investigated so far; thus, older users need to be explicitly considered in empirical investigations (Garg et al. 2012).

Importantly, previous user studies on cybersecurity did not consider the effect of the content of phishing emails on their effectiveness (Benenson et al. 2017; Halevi et al. 2015; Jagatic et al. 2007; Mohebzada et al. 2012; Uebelacker and Quiel 2014; but see Butavicius et al. 2016). One exception is a study by Ferreira and Lenzini (2015) that used qualitative content analysis to identify five weapons of influence in phishing emails (i.e., authority, social proof, liking/similarity/deception,

commitment/reciprocation/consistency, and distraction). Also, using a semi-structured interview, Whitty (2013) found that similar weapons of influence were commonly used in online dating romance scam. However, these previous qualitative studies did not determine the relative effectiveness of specific principles of persuasion in luring users to fall for attacks. Uebelacker and Quiel (2014) proposed a theoretical model attempting to link weapons of influence used in phishing to personality traits of individuals who had fallen for attacks. However, as of yet, their theoretical framework has not been empirically supported. This lack of a solid body of empirical work is particularly surprising, considering that certain phishing emails are more convincing than others. To systematically address variations in effectiveness, the present study manipulated the phishing email content. In particular, we created a set of simulated phishing emails that varied in weapons of influence and life domains and examined young and older users' susceptibility as a function of these email content characteristics.

Next, we review the literature on trust and susceptibility in aging. We then introduce the two main concepts, weapons of influence and life domains as two factors that we propose to contribute to the effectiveness of phishing emails.

2.2 Trust and Susceptibility in Aging

Despite a lack of direct investigation into susceptibility, multiple lines of research provide support for the hypothesis that older adults may be more susceptible to phishing than young adults. For example, as individuals age, perceived trust increases (Zebrowitz et al. 2017, 2013), while sensitivity to untrustworthy information declines (Castle et al. 2012; Ebner et al. 2015; Ruffman et al. 2012). Furthermore, older compared to young adults were more likely to show trust in interaction with others (e.g., more generous investment in trust games; Bailey et al. 2013, 2015, 2016). These findings are in line with the well-documented age-related positivity bias and more specifically reduced attention and memory to negative relative to positive information in aging (Carstensen and Mikels 2005; Mather and Carstensen 2005; Reed et al. 2014). Also, older compared to young adults showed impaired ability in recognizing lies and had difficulty discriminating between trustworthy and untrustworthy faces (Castle et al. 2012; Ruffman et al. 2012). Furthermore, older compared to young adults showed reduced brain activation in insula to cues of untrustworthiness (Castle et al. 2012). In addition, older adults who had experienced financial exploitation in real life showed reduced cortical thickness in anterior insula when compared with individuals who had experienced attempts for financial exploitation but had not fallen for it (Spreng et al. 2016). Together, these findings suggest that age-related cognitive and functional brain changes contribute to an age-related decrease in sensitivity to untrustworthy information (see also Ebner et al. 2018; Gavett et al. 2017). Older compared to young adults may focus on potential gains proposed in phishing emails and may overlook cues of deception, rendering them more susceptibility to such attacks. This hypothesis is also supported by above-referenced evidence that reliance on deliberative processing during decision making decreases with age (Jones et al. 2019; Peters et al. 2007).

In addition, age-related change in personality may make older compared to young adults more susceptible to phishing. Both cross-sectional and longitudinal evidence suggests an increase in conscientiousness with age (Helson and Kwan 2000; Terracciano et al. 2005). Previous work has shown that individuals with higher conscientiousness were more susceptible to phishing (Halevi et al. 2015). Thus, greater conscientiousness with age may render older adults more susceptible to phishing. A recent study found that older adults with a personality trait to trust things that are unproven or unlikely to be true (i.e., credulity; Pinsker et al. 2010) were more likely to be persuaded and fall for fraud (Shao et al. 2019). Thus, older adults may be more likely to believe the information in phishing emails and to become victims of phishing.

Furthermore, it is plausible that older compared to young adults may be more persistent in their susceptibility to phishing. This assumption is based on evidence from a recent study showing that, in a trust game, older adults maintained high evaluations of trustworthiness for their partners (i.e., trustee in the game) even after they experienced those partners to breach their trust (Suzuki 2016). In contrast, young adults more readily adjusted their trustworthiness evaluations based on their partners' behavior. This reduced adjusting of trustworthiness evaluations in older adults is in line with research showing that age reduced the ability to update the value of objects in response to online feedback about the objects (Eppinger et al. 2011; Samanez-Larkin and Knutson 2015). Therefore, it is possible that older compared to young adults are more persistent in their susceptibility to phishing and show less adjustment in their trusting behavior over time.

Considering the above evidence, the present research set out to address the following research question (*Q1*): *Do young and older Internet users differ in their susceptibility to phishing emails?* To address this question we tested the following hypotheses: (*H1a*) *Compared to young users, older users will be particularly susceptible to phishing emails.* (*H1b*) *Young users will show a decrease in their susceptibility to phishing emails as the study proceeds, while older users' susceptibility will persist throughout the study.*

2.3 Principles (Weapons) of Influence

Humans often apply heuristics that can be beneficial in promoting fast and frugal actions, but can also result in faulty decision-making (Ferreira and Lenzini 2015; Gigerenzer and Gaissmaier 2011; Kahneman and Egan 2011; Pachur et al. 2017). In the context of persuasion, Cialdini (2007) proposed that humans have fixed behavioral patterns triggered by certain events, which may be considered the psychological correlate of sensorimotor reflexes. These triggered patterns of behavior can be effective for decision-making, but they can also be exploited by adversaries to lure individuals into a behavior that counter their best interest. Cialdini called the events triggering these behavioral patterns *psychological principles of influence*. He defined six principles (called *weapons of influence* in this article): *authority, commitment, liking, reciprocation, scarcity*, and *social proof*. A seventh principle, *perceptual contrast*, serves similar functions and was added based on Hadnagy's work on social engineering (Hadnagy 2010).

The principle of *authority* states that humans tend to comply with requests made by figures of authority, such as law enforcement personnel, lawyers, doctors, or politicians. Therefore, sending emails in the name of known authorities may be effective in luring recipients into clicking on a malicious link in an email.

The *commitment* principle proposes that once humans have taken a stand, they feel pressured to behave consistently with that stance. For example, Alice as the mother of two college students may feel devastated every time she learns about a new case of campus violence. Observing this, an adversary can target Alice by sending her an email asking her to click on a link to support a program to prevent campus violence.

The *liking* principle assumes that humans tend to comply with requests from people they like or with whom they share similarities. Consider Mary, an older adult who is also active in her local church. Per the liking principle, she will feel more at ease accepting a request from Dan, who is her age contemporary and is also a member of the same church, than a request from John, who is much young and attends a local university.

The *perceptual contrast* principle refers to the way people perceive the relative difference between two things that are presented in tandem. When the first is perceived as relatively worse than the second, people tend to perceive the second as better than it actually is. For example, a car salesperson may present the most expensive car in the lot first, whereby the subsequent car prices may seem more reasonable to the buyer than they would have been otherwise. The salesperson

never intended to sell the first car, but wanted to sell the second car at a price that the buyer would not have otherwise considered. That is, with perceptual contrast, the attacker introduces a bias into the victim's perception of the intrinsic value or cost of an action based on its relation to the initially presented option.

The *reciprocation* principle is based on the notion that humans tend to repay, in kind, what another person has provided them. An adversary can use this principle to lure a user into installing malware on a computer by offering a free gift attached (e.g., a pdf for a travel guide).

The principle of *scarcity* proposes that the perceived value of an object, experience, or opportunity is greatly increased when its availability is limited. Therefore, an adversary may tempt a user into clicking on a malicious link or website to get a "soon-to-expire" discount.

Finally, the *social proof* principle leverages the human tendency to avoid mistakes by acting according to what the majority of other people are doing. An adversary can exploit this principle by advertising, via a malicious link, an offer from a company "voted" as one of the top 10 in the country.

No previous study has systematically compared the relative effectiveness of these seven weapons of influence on phishing or has looked at age differences in their effectiveness. We, therefore, posed two research questions relevant to weapons of influence: (*Q2a*) *Which weapon*(*s*) *of influence is/are particularly effective*? (*Q2b*) *Does the relative effectiveness of weapons of influence vary between young and older users*? Given the lack of previous research, we did not formulate directional hypotheses regarding the relative effectiveness of weapons of influence.

2.4 Life Domains

To increase their impact on recipients, adversaries can construct a phishing email within a particular life domain context. Personal relevance of specific life domains varies by demographics and differs from person to person. In the present study, we adopted Baltes' lifespan development theoretical framework (Baltes 1987) and considered six life domains phishing emails can refer to *financial, health, ideological, legal, security*, and *social*.

Financial emails focus on money, discounts, or offers (e.g., an email offering a discounted vacation package). *Health* emails focus on mental and physical wellness, including sports and medication (e.g., an email offering a medication). *Ideological* emails focus on principles and beliefs (e.g., an email inviting someone to sign a petition). *Legal* emails focus on the law, such as emails about being arrested or sued, or an invitation to appeal a parking ticket. *Security* emails focus on safety, such as neighborhood watch or cybersecurity (e.g., an email invite to explore the Facebook page of a neighborhood). Finally, *social* emails focus on social interaction (e.g., an email inviting an individual to learn more about an upcoming concert in town).

Life-span developmental theory states that the relevance of specific life domains changes with age because individuals at different points in their lifespan pursue different goals (Baltes 1987; Ebner et al. 2006). In particular, within the meta-theoretical framework of life-span theory Socioemotional Selectivity Theory posits that the priority of personal goals changes as people age (Carstensen et al. 1999; Isaacowitz 2006; Mather and Knight 2005), with older adults showing greater prioritization of social over information-seeking goals (Fredrickson and Carstensen 1990; Fung, Carstensen and Lang 2001). Further, older compared to young adults may be particularly interested in information relevant to health, as they experience a variety of health issues (Oh and Cho 2015; Flynn et al. 2006). Similar to weapons of influence, no previous study has systematically investigated the relative effectiveness of phishing emails focusing on these six life domains or has looked at age differences in their effectiveness. We therefore posed two research questions relevant to life domains: (*Q3a*) *Which life domain*(*s*) *is/are particularly effective*? (*Q3b*) *Does the relative effectiveness of life domains vary between young and older users*? Given the lack of previous

research, we did not formulate directional hypotheses regarding the relative effectiveness of life domains.

2.5 Susceptibility Awareness

In addition to actual behavioral susceptibility to phishing emails, we were also interested in exploring age differences and effectiveness of weapons of influence and life domains in susceptibility awareness to phishing emails (i.e., the self-reported likelihood of users to click on the links embedded in phishing emails). Based on above reported evidence that age is associated with increased perceived trust (Zebrowitz et al. 2013, 2017), while sensitivity to untrustworthy information declines with age (Castle et al. 2012; Ebner et al. 2015; Ruffman et al. 2006; 2012), we posed the following research questions regarding susceptibility awareness: (*Q4a*) *Do young and older Internet users differ in their susceptibility awareness to phishing emails*? (*Q4b*) *Does susceptibility awareness vary by weapon(s) of influence and does age moderate this variability*? (*Q4c*) *Does susceptibility awareness vary by life domain(s) and does age moderate this variability*?

3 THE PRESENT STUDY

To address our research questions, we conducted a user study over a period of 21 days, which took place at the participants' homes for increased ecological validity and allowed us to assess susceptibility to phishing emails behaviorally. During the 21-day study period, unbeknownst to them, we exposed young and older Internet users to experimentally controlled simulated phishing emails, which varied on the use of weapons of influence and life domains. Participants' Internet activities on the computer they had registered for the study were monitored over the 21 study days via a pre-installed browser extension (plugin), which recorded (with participants' consent) all URLs the participants visited during the study period, including URLs embedded in our simulated phishing emails. The clicking on the links in our simulated emails indicated that the participant would have fallen for the attack had it been real. Further, to assess susceptibility awareness to the phishing emails, on the last study day users reviewed 21 simulated phishing emails that they had not seen during the study intervention and indicated how likely they would click on the link in each email.

4 METHODS

4.1 Participants

Our study comprised of 100 young (M = 21.7 years, SD = 4.1, 56.0% female) and 58 older (M = 61.7 years, SD = 6.8, 43.1% female) users. Table 1 summarizes participants' demographics, health, and Internet usage by age group. Participants were recruited from North Central Florida via fliers (18 participants), handouts (10 participants), newspaper ads (10 participants), a lab-internal participant pool (12 participants), the university participant pool (58 participants), HealthStreet (a university-affiliated community recruitment and outreach program; 16 participants), and online venues (e.g., Facebook, Craigslist, ResearchMatch.org; 5 participants), and other mechanisms (e.g., word of mouth; 29 participants). Young participants recruited through the university participant pool were compensated with course credit; all other participants were compensated with a $50 gift card.

For inclusion in the data analysis, participants needed to complete 21 days of study intervention and have at least 50% recorded daily email checking activities (see details below). These criteria excluded 33.1% (n = 78) of the total 236 volunteers originally enrolled. Excluded individuals were equally distributed across age group and gender. Among participants who did not complete the study, 22 gave an explicit reason for their discontinuation: Nine dropped out due to insufficient

Table 1. Demographic, Health, and Internet Usage Information in Young and Older Participants

	Young M (SD)/%	Older M (SD)/%	Age-group differences
Years of education ($n_{young} = 81, n_{older} = 33$)	14.24 (3.57)	16.30 (2.79)	$t(122) = -2.97$
Annual income ($n_{young} = 91, n_{older} = 54$)			
<$40,000	36.3	33.3	
$40,000–$70,000	0.0	31.5	$\chi^2(3) = 61.83$
>$70,000	0.0	18.5	
N/A	63.7	16.7	
Race/ethnicity ($n_{young} = 91, n_{older} = 52$)			
American Indian or Alaskan Native	0.0	5.8	
Asian	29.7	1.9	
Black/African American	8.8	9.6	$\chi^2(5) = 36.68$
Native Hawaiian	0.0	1.9	
Hispanic	19.8	1.9	
White	39.6	76.9	
Physical health ($n_{young} = 91, n_{older} = 52$)	7.69 (1.56)	7.58 (1.95)	$t(141) = 0.39$
Mental health ($n_{young} = 91, n_{older} = 52$)	8.02 (1.53)	8.54 (1,50)	$t(141) = 1.86$
Marital status ($n_{young} = 91, n_{older} = 53$)			
Single	68.1	15.1	
In a relationship, but not married	26.4	15.1	
Married	4.4	47.2	$\chi^2(4) = 69.09$
Divorced/separated	1.1	15.1	
Widowed	0.0	7.5	
Internet usage/week ($n_{young} = 81, n_{older} = 49$)			
≤4 hours	21	20.4	
4–9 hours	34.6	44.9	$\chi^2(2) = 1.56$
≥10 hours	44.4	34.7	
Average number of URLs visited/day ($n_{young} = 99, n_{older} = 57$)	256.46 (166.14)	181.52 (115.85)	$t(154) = 3.01$

Note. Participants with negligible income/unemployed reported "N/A". Physical Health "*Please rate your general physical health*" and Mental Health "*Please rate your general mental health/mood*" were measured by single self-report items on a scale ranging from 1 = *poor* to 10 = *excellent*.

time for completing the study; ten experienced technical difficulties (e.g., plugin installation, audio response recording); and three became suspicious of the nature of the study.

4.2 Procedure

The university IRB approved the study protocol. We determined study eligibility through a brief phone interview, after informed verbal consent. To be eligible, participants had to be between 18 and 39 years (young participants) or 60 and 90 years (older participants). Eligible participants needed to engage in online activities (e.g., web browsing, email checking) regularly, but not necessarily daily. In addition, older users received the Telephone Interview for Cognitive Status

(TICS; Brandt et al. 1988) to screen for cognitive impairment (cut off score < 30). We also administrated the Brief Test of Adult Cognition by Telephone (BTACT; Tun and Lachman 2006) to measure various cognitive abilities (see Ebner et al. 2018 for details).

For eligible participants, informed written consent was obtained via an online form, disclosing study procedures, the minimal study risk, and data protection mechanisms.[2] To ensure naturalistic behavior, participants were told that the purpose of the study was to examine daily Internet use. Participants were not informed about the simulated phishing emails until debriefing at study closure. Next, with the help of a video tutorial and as needed instructions over the phone, participants installed a plugin that allowed the recording of all URLs participants visited during the study, consequently recording whether participants clicked on the link embedded in each stimulated phishing email from the PHIT (see details in the Appendix). Each link embedded in each simulated phishing email was accompanied by a façade web page created for this study (see the Appendix for details). Clicking on the link embedded in the phishing emails constituted our central dependent variable, *susceptibility to phishing emails*.

On the first day of the 21-day intervention, participants filled out a demographic questionnaire via an online survey. Using an online survey link, on each study day, participants also completed the short Positive and Negative Affective Schedule (PANAS; Watson et al. 1988) to access their daily mood before they engaged in the PHIT. For the PHIT, participants were asked to spend one hour of study-related Internet activities daily. These activities included: (i) reading an informative source (e.g., a news media website), (ii) reading entertainment/social network sources (e.g., Facebook), (iii) engaging in unstructured browsing, and (iv) time checking/handling emails from the email account the user had registered with for the study, with 15 minutes on each of these tasks. This variety of study-related activities assured capture of a range of possible everyday computer use, and most importantly, assured a sufficient base rate of email checking during the study period. During the 21-day study period, unbeknownst to them, participants received 21 simulated phishing emails (one per day) in the email account they had registered for the study (see the Appendix for details). A *Phishing Manager* was developed for this study and used to send the simulated phishing emails. This system was managed via five time-based process schedulers.

On the last study day, participants were asked to review 21 simulated phishing emails which they had not seen during the study intervention but which were comparable to the ones they had seen (see details below about counterbalancing). Participants were asked to evaluate, for each of these emails, how likely they would click on the link in the email (i.e., likelihood), how interested they were in what each email had to say (i.e., interested), and how convincing they found the content of the email (i.e., convincing). Participants used a 5-point scale (1 = *not at all*, 5 = *very much*) for their responses. We used self-reported likelihood of clicking on an email link as an indicator of users' susceptibility awareness (e.g., higher self-reported likelihood of clicking on the link suggested higher susceptibility awareness). In addition, participants also completed a survey to measure socio-emotional functions including trust, state anxiety, and trait anxiety (see Ebner et al. 2018 for details). During the debriefing, we disclosed the true purpose of the study. As part of the debriefing process, we asked participants about their thoughts regarding the study purpose and the need to use deception. Ninety-nine percent of the participants indicated that they understood the necessity of concealing the true study purpose.

[2]Upon consent, participants were assigned a study ID, which served as participant identifier; any personal information was stored separately as per the university IRB.

4.3 Model Specification

Accommodating for the hierarchical structure of the data (i.e., email clicks nested within participants), we conducted three multilevel logistic regression models to address our research questions. Susceptibility, operationalized as the clicking on an email link during the 21-day study period (0 = not clicked, 1 = clicked), served as dichotomous outcome variable in all three models. The first multilevel logistic regression model tested the extent to which susceptibility differed between young and older users ($Q1a–b$). This model used age group (categorical variable; 0 = young, 1 = older), gender (categorical variable; 0 = male, 1 = female), time in study (continuous variable; range: 1–21), and the interactions between these variables as predictors.

The second multilevel logistic regression model tested the extent to which susceptibility varied as a function of the weapons of influence in young and older users ($Q2a–b$). This model used age group, gender, weapons of influence (categorical variable: 1 = Authority, 2 = Commitment, 3 = Liking, 4 = Perceptual Contrast, 5 = Reciprocation, 6 = Scarcity, 7 = Social Proof), and the interactions between these variables as predictors.

The third multilevel logistic regression model tested the extent to which susceptibility varied as a function of life domains in young and older users ($Q3a–b$). This model used age group, gender, life domains (categorical variable: 1 = Financial, 2 = Health, 3 = Ideological, 4 = Legal, 5 = Security, 6 = Social), and the interactions between these variables as predictors.

In an exploratory fashion, we conducted two multilevel regression models to test the susceptibility awareness as a function of age group, gender, weapons of influence, and life domains ($Q4a–c$). In these two models, susceptibility awareness, operationalized as the self-reported likelihood of clicking rating (1 = *not at all*, 5 = *very much*), served as continuous outcome variable. The first multilevel regression model tested the extent to which susceptibility awareness varied as a function of weapons of influence and considered the moderation of age group and gender. In particular, this model used age group, gender, weapons of influence, and the interactions between these variables as predictors. The second multilevel regression model tested the extent to which susceptibility awareness varied as a function of life domains and considered the moderation of age group and gender. That is, this model used age group, gender, life domain, and the interactions between these variables as predictors.

In all five models, the Wald statistics was used to indicate the significance of each effect. Adopting a top-down approach (i.e., from higher-order interaction to main effects), we removed nonsignificant effects from each model to determine the most parsimonious model to reflect the data. We used Stata 14.0 for all statistical analyses and applied $p = 0.05$ as the significance threshold.

5 RESULTS

Overall, susceptibility to phishing was high, with 43.3% of users clicking on at least one of the 21 simulated phishing email links and 11.9% of users clicking on more than one link during the 21-day study period.

5.1 Q1a-b: Susceptibility in Young and Older Internet Users

The interaction between age group, gender, and time in study ($\chi^2(1) = 2.92, p = 0.09$) and the interaction between gender and time in study ($\chi^2(1) = 3.53, p = 0.06$) were marginally significant. The interactions between age group and gender ($\chi^2(1) = 5.41, p = 0.02$) and between age group and time in study ($\chi^2(1) = 4.77, p = 0.03$) were significant, suggesting that the age-group difference in susceptibility varied depending on the participants' gender and their time in the study (Table 2). The main effect of time in study ($\chi^2(1) = 14.76, p < 0.001$) was also significant, but

Table 2. Results of Multilevel Logistic Regression Model for Susceptibility to Phishing as a Function of Age Group, Gender, and Time in Study (Q1a-b)

Fixed effects	B (SE)	Odds ratio
Age group	−1.21(0.46)	0.3
Gender	−0.36(0.29)	0.7
Time in study	**−0.1(0.03)**	**0.9**
Age group × gender	**0.98(0.49)**	**2.68**
Age group × time in study	**0.09(0.04)**	**1.09**
Random effects	Variance (SE)	
Intercept	**0.35(0.2)**	

Notes. Dependent variable: Susceptibility (0 = not clicked, 1 = clicked). The final model included age group (0 = young, 1 = older), gender (0 = male, 1 = female), time in study, the interaction between age group and gender, and the interaction between age group and time in study as independent variables. Bold print indicates significant effects at $p < 0.05$.

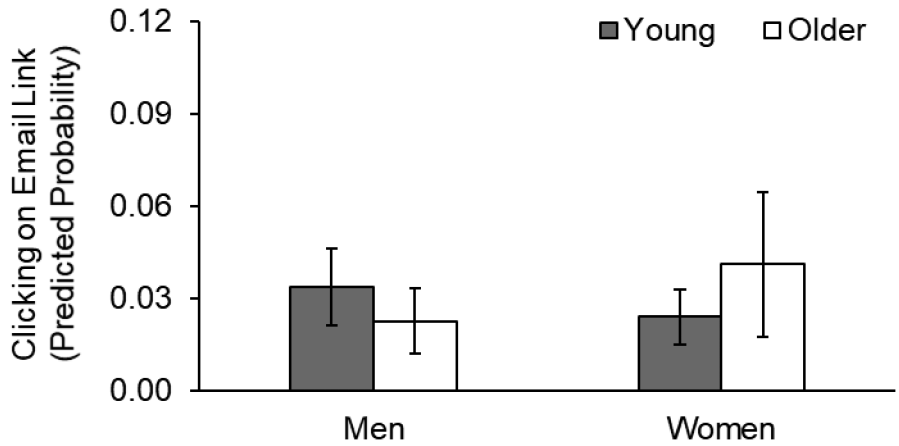

Fig. 1. Predicted susceptibility to phishing in young and older men and women. Error bars represent 95% confidence intervals.

the main effects of age group ($\chi^2(1) = 2.49, p = 0.11$) and gender ($\chi^2(1) = .29, p = 0.59$) were not significant.

In sum, as shown in Figure 1, older women (4.1%) constituted the most susceptible group to the simulated phishing emails compared to the other demographics (young men: 3.4%, young women: 2.4%, older men: 2.3%). Also, as shown in Figure 2, young users' susceptibility declined with time in the study, while in older users' susceptibility remained stable over the study period.

5.2 Q2a-b: Susceptibility as a Function of Weapons of Influence in Young and Older Users

The interaction between age group, gender, and weapons of influence ($\chi^2(5) = 1.33, p = 0.93$) and the interaction between gender and weapons of influence ($\chi^2(6) = 8.37, p = 0.21$) were not significant. The interaction between age group and weapons of influence was significant ($\chi^2(6) =$

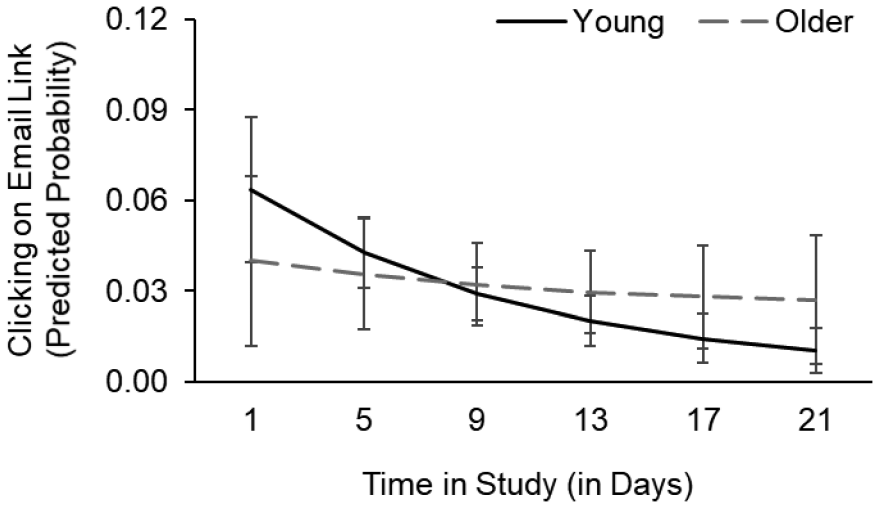

Fig. 2. Predicted susceptibility to phishing in young and older users as a function of time in study (in days). Error bars represent 95% confidence intervals.

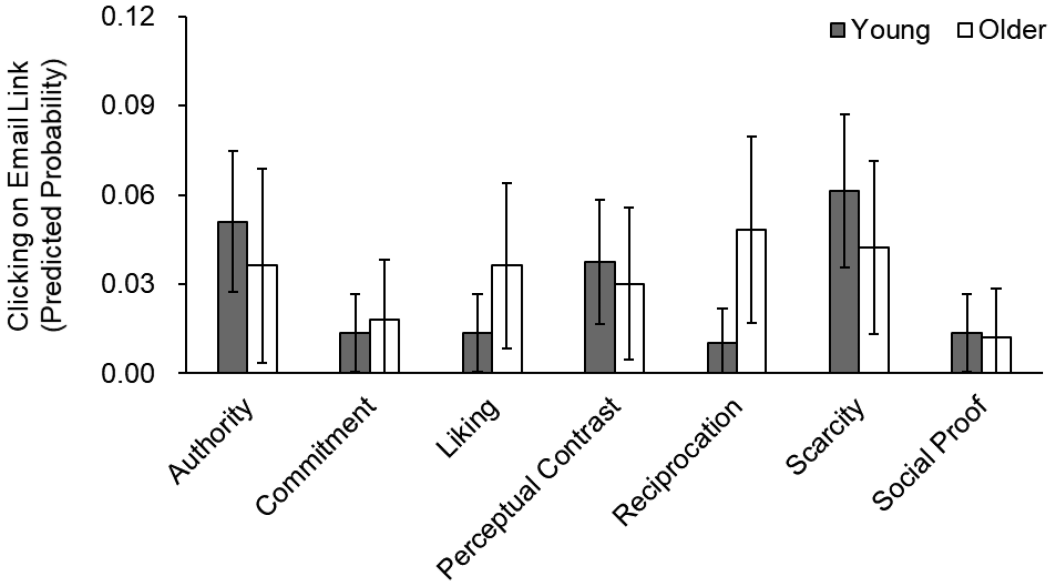

Fig. 3. Predicted susceptibility to phishing as a function of weapons of influence in young and older users. Error bars represent 95% confidence intervals.

$12.61, p = 0.05$), suggesting that young and older users differed in their susceptibility to specific weapons of influence. The interaction between age group and gender was also significant ($\chi^2(1) = 6.37, p = 0.01$). In addition, the main effect of weapons of influence was significant ($\chi^2(6) = 26.18, p < 0.001$), suggesting that users differed in their susceptibility to phishing depending on the specific weapons of influence applied (Table 3).

In particular, as shown in Figure 3 users were significantly more likely to click on links in emails using scarcity (5.3%) than those using reciprocation (2.3%), liking (2.1%), commitment (1.5%), and

Table 3. Results of Multilevel Logistic Regression Model for Susceptibility to Phishing as a Function of Age Group, Gender, and Weapons of Influence (Q2a-b)

Fixed effects	*B* (*SE*)	Odds ratio
Age group	−0.9 (0.5)	0.41
Gender	−0.36 (0.29)	0.70
Age group × gender	**0.99 (0.49)**	**2.69**
Weapons of influence (vs. authority)		
Commitment	**−1.38 (0.58)**	**0.25**
Liking	**−1.38 (0.58)**	**0.25**
Perceptual contrast	−0.33 (0.39)	0.72
Reciprocation	**−1.67 (0.57)**	**0.19**
Scarcity	0.2 (0.32)	1.22
Social proof	**−1.38 (0.52)**	**0.25**
Age group × weapons of influence (vs. authority)		
Older × commitment	0.65 (0.91)	1.92
Older × liking	1.38 (0.81)	3.96
Older × perceptual contrast	0.14 (0.63)	1.15
Older × reciprocation	**1.98 (0.78)**	**7.21**
Older × scarcity	−0.03 (0.72)	0.97
Older × social proof	0.24 (0.82)	1.27
Random effects	Variance (SE)	
Intercept	**0.37 (0.21)**	

Notes. Dependent variable: Susceptibility (0 = not clicked, 1 = clicked). The final model included age group (0 = young, 1 = older), gender (0 = male, 1 = female), weapons of influence (reference category = authority), the interaction between age group and gender, and the interaction between age group and weapons of influence as independent variables. Bold print indicates significant effects at $p < 0.05$.

social proof (1.3%). Also, users were significantly more susceptible to emails using authority (4.4%) than those using commitment and social proof. In addition, perceptual contrast (3.4%) was significantly more effective than social proof. Furthermore, young users showed greater susceptibility to scarcity (young = 6.1%, older = 4.2%) and, to a lesser extent, authority (young = 5.1%, older = 3.6%) than older users. In contrast, older users showed greater susceptibility to reciprocation (young = 1.0%, older = 4.8%) and, to a lesser extent, liking (young = 1.4%, older = 3.6%) than young users.

5.3 Q3a-b: Susceptibility as a Function of Life Domains in Young and Older Users

The interaction between age group, gender, and life domains was not significant ($\chi^2(5) = 0.60, p = 0.99$). In addition, the interactions between age group and life domains ($\chi^2(5) = 2.31, p = 0.81$) and between gender and life domains ($\chi^2(5) = 5.35, p = 0.37$) were not significant. The interaction between age group and gender was marginally significant ($\chi^2(1) = 3.35, p = 0.07$), and when we removed from the model the non-significant interactions between age group and life domains and between gender and life domain, the interaction between age group and gender was significant ($\chi^2(1) = 4.09, p = 0.04$). The main effect of life domains was also significant ($\chi^2(5) = 43.73, p < 0.001$), suggesting that users differed in their susceptibility to phishing depending on the specific life domains the attack applied (Table 4).

As shown in Figure 4, users showed greater susceptibility to legal emails (6.7%) than emails in any other life domain. Susceptibility was also greater for ideological emails (3.2%) than

Table 4. Results of Multilevel Logistic Regression Model for Susceptibility to Phishing as a Function of Age Group, Gender, and Life Domains (Q3a-b)

Fixed effects	B (SE)	Odds ratio
Age group	−0.42 (0.32)	0.66
Gender	−0.36 (0.29)	0.70
Age group × gender	**1.00 (0.49)**	**2.71**
Life domains (vs. financial)		
Health	0.87 (0.46)	2.39
Ideological	**1.13 (0.47)**	**3.09**
Legal	**1.91 (0.44)**	**6.73**
Security	0.52 (0.53)	1.68
Social	0.61 (0.52)	1.85
Random effects	Variance (SE)	
Intercept	**0.36 (0.21)**	

Notes. Dependent variable: Susceptibility (0 = not clicked, 1 = clicked). The final model included age group (0 = young, 1 = older), gender (0 = male, 1 = female), life domains (reference category = financial), and the interaction between age group and gender as independent variables. Bold print indicates significant effects at $p < 0.05$.

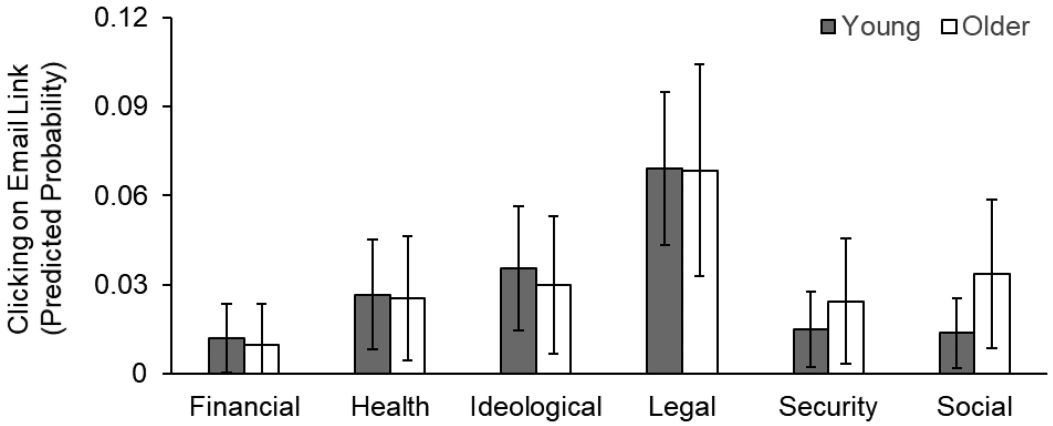

Fig. 4. Predicted susceptibility to phishing as a function of life domains in young and older users. Error bars represent 95% confidence intervals.

financial emails (1.1%). Susceptibility to health (2.5%), security (1.8%), and social (2.0%) emails was comparable and was not significantly different from either financial or ideological emails. This pattern of findings was equivalent across young and older users.

5.4 Q4a-c: Susceptibility Awareness as a Function of Weapons of Influence/Life Domains in Young and Older Users

The interaction between age group, gender, and weapons of influence ($\chi^2(6) = 7.84, p = 0.25$) was not significant. In addition, the interactions between age group and gender ($\chi^2(1) = 0.33, p = 0.57$), age group and weapons of influence ($\chi^2(6) = 8.19, p = 0.22$), and gender and weapons of influence ($\chi^2(6) = 10.63, p = 0.10$) were not significant. The main effect of gender was also

Table 5. Results of Multilevel Regression Model for Susceptibility Awareness to Phishing as a Function of Age Group, Gender, and Weapons of Influence (Q4a-b)

Fixed effects	B (SE)
Age group	**−0.6 (0.32)**
Gender	0.02 (0.29)
Weapons of influences (vs. authority)	
Commitment	0.08 (0.11)
Liking	**−0.29 (0.08)**
Perceptual contrast	**−0.26 (0.09)**
Reciprocation	−0.14 (0.09)
Scarcity	−0.12 (0.08)
Social proof	**−0.47 (0.08)**
Random effects	Variance (SE)
Intercept	**3.29 (1.22)**

Notes. Dependent variable: Susceptibility awareness. The final model included age group (0 = young, 1 = older), gender (0 = male, 1 = female), and weapons of influence (reference category = authority) as independent variables. Bold print indicates significant effects at $p < 0.05$.

not significant ($\chi^2(6) = 10.63, p = 0.10$). The main effect of weapons of influence was significant ($\chi^2(6) = 78.03$, $p < 0.001$; Table 5); users showed the highest susceptibility awareness for emails using authority (2.11). Susceptibility awareness for authority emails was higher than susceptibility awareness of emails using any of the other weapons of influence except scarcity. In addition, users showed higher susceptibility awareness for emails using scarcity (2.03) and commitment (1.91) than for emails using perceptual contrast (1.75), reciprocation (1.78), and social proof (1.56). Susceptibility awareness for emails using social proof was the lowest and was lower than susceptibility awareness for emails using any of the other weapons of influence (Figure 5A).

The interaction between age group, gender, and life domains ($\chi^2(5) = 5.50, p = 0.36$) was not significant. In addition, the interactions between age and gender ($\chi^2(1) = 0.33, p = 0.56$), age group and weapons of influence ($\chi^2(5) = 9.11, p = 0.10$), and gender and weapons of influence ($\chi^2(5) = 3.85, p = 0.57$) were not significant. In contrast, the effect of life domains was significant ($\chi^2(5) = 13.61$, $p = 0.02$; Table 6). That is, users showed the highest susceptibility awareness for legal emails (2.04) and susceptibility awareness for legal emails was significantly higher than susceptibility awareness for financial (1.83), security (1.79), and health (1.74) emails (Figure 5B).

Finally, the main effect of age group was significant in both models ($\chi^2(1) = 3.59$, $p = 0.058$ and $\chi^2(1) = 3.60$, $p = 0.058$, respectively). That is, older users showed lower susceptibility awareness than young users.

6 DISCUSSION

By adopting a method with high ecological validity and by using a pool of simulated phishing emails, which systematically manipulated email content pertaining to weapons of influence and life domains, the present study examined susceptibility to phishing in young and older users and determined the extent to which susceptibility varied as a function of weapons of influence and life domains. The study generated several novel findings as discussed in the following.

First, we observed a high overall susceptibility to phishing, as more than 40% of users clicked on the link in at least one of the simulated phishing emails during the 21-day study period. Note

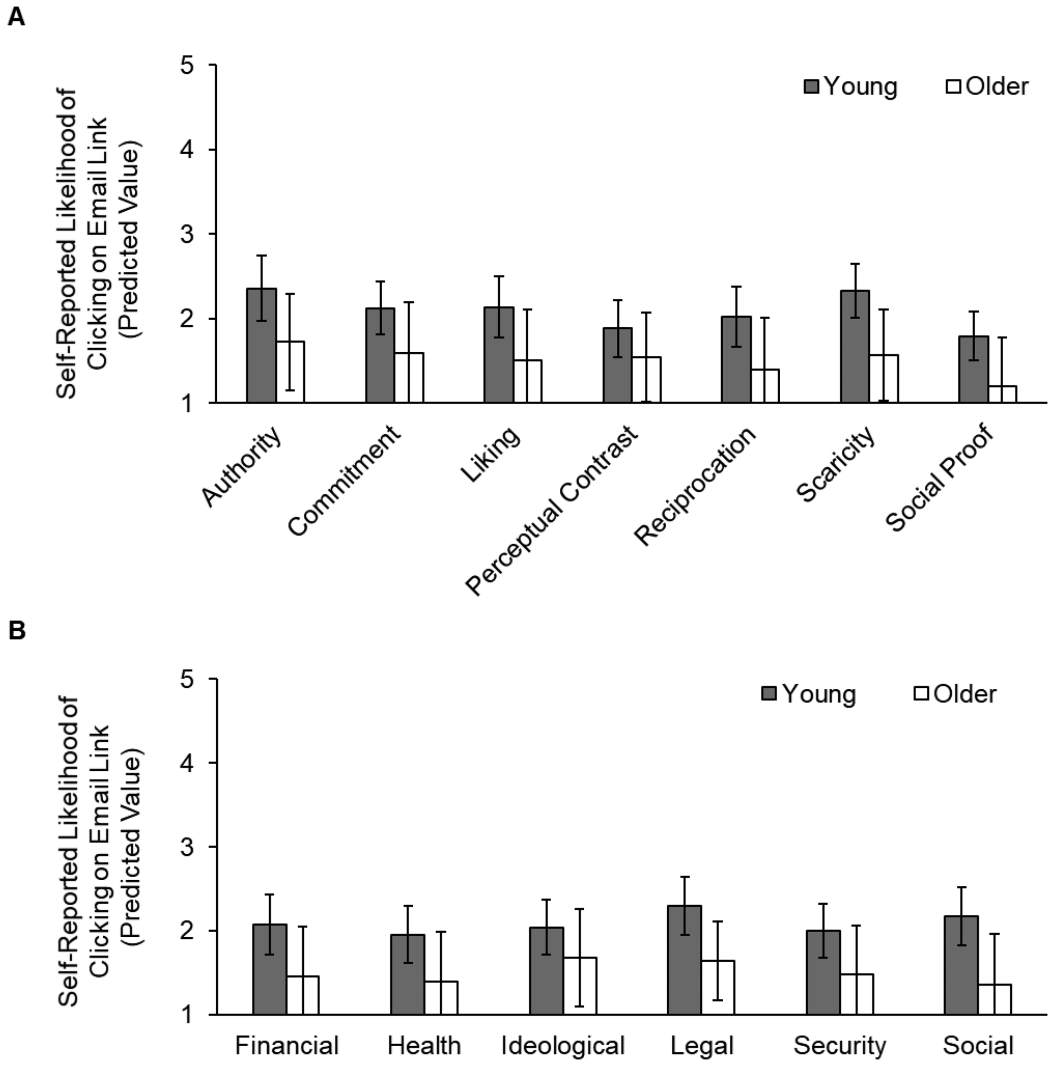

Fig. 5. Predicted susceptibility awareness to phishing as a function of (A) weapons of influence and (B) life domains in young and older users. 1 = not at all; 5 = very much. Error bars represent 95% confidence intervals.

that clicking on one phishing email can affect an individual's computer and through that computer multiple other computers. In line with our findings, Benenson et al. (2017) observed that 20% of email users and 43% of Facebook users clicked on simulated phishing links. Suggesting even higher susceptibility, Jagatic et al. (2007) found a high success rate (72%) of simulated phishing emails (seemingly sent from known acquaintances) among college students. Similarly, Halevi et al. (2015) observed that more than 62% of employees fell for simulated phishing emails they believed were sent from their company's IT manager. Participants in the present study received simulated phishing emails from unknown entities/others (e.g., local farmers market, parking authority). This methodological variability between studies may explain differences in susceptibility rates.

Table 6. Results of Multilevel Regression Model for Susceptibility Awareness to Phishing as a Function of Age Group, Gender, and Life Domains (Q5a-b)

Fixed effects	B (SE)
Age group	−0.60 (0.32)
Gender	0.02 (0.29)
Life domains (vs. financial)	
Health	−0.15 (0.09)
Ideological	**−0.31 (0.08)**
Legal	−0.18 (0.09)
Security	**−0.25 (0.08)**
Social	**−0.21 (0.08)**
Random effects	Variance (SE)
Intercept	**3.29 (1.22)**

Notes. Dependent variable: Susceptibility awareness. The final model included age group (0 = young, 1 = older), gender (0 = male, 1 = female), and life domains (reference category = financial) as independent variables. Bold print indicates significant effects at $p < 0.05$.

Some previous studies reported lower susceptibility than found in our research. For example, Mohebzada et al. (2012) observed very low susceptibility across two large-scale phishing experiments. In their study, phishing emails were sent to 10,917 institutional email addresses, associated with students, alumni, faculty, and staff from a specific university. The success rate of phishing was about 9% in their first experiment and 2% in their second experiment. Of note, about half of the email addresses targeted in Mohebzada et al. were from alumni, for whom it was not clear if they still checked their university email inbox regularly. Thus, it is possible that the actual number of individuals who saw the simulated phishing emails was smaller than 10,917. In the present study, phishing emails were sent to participants personal email inbox of the account they had registered with in the study. In addition, participants were asked as part of the study to engage in daily Internet activities, including checking their emails. These design features were implemented to increase the likelihood that participants would actually see the simulated phishing emails. Also, Mohebazada et al. defined susceptibility as either inputting correct personal credentials (in Experiment 1) or as completing an online survey (in Experiment 2). This operationalization of susceptibility was different (and representative of not just falling for an attack in the form of clicking on a link but actually providing personal information) from the measure used in the present study (i.e., clicking on the link embedded in the simulated phishing email). This difference in operational definition of susceptibility across the two studies may explain the different susceptibility rates. Finally, Mohebazada et al. only used one phishing email (per experiment) and their observation window was short (i.e., 10 days in Experiment 1; 18 hours in Experiment 2)—compared to our 21-day study intervention in which 21 phishing emails were sent—which may also have contributed to the low susceptibility rate in their investigation.

The high susceptibility to phishing found in our study, in line with similarly high or higher susceptibility reported in previous work, emphasizes the significant threat posed by phishing emails and warrants the development of efficient detection and prevention tools as well as effective phishing education protocols. Intriguingly, in contrast to this overall high (behavioral) susceptibility in

the present study, participants' self-reported susceptibility awareness was low. This disparity between behavior and self-report was especially pronounced among older users and highlights the importance of behavioral field experiments (vs. self-report) to study susceptibility to phishing, especially among older adults. The lower susceptibility awareness in older than young users observed in our study is in line with evidence of increased trust perceptions and decreased sensitivity to cues of untrustworthiness in older relative to young adults (Castle et al. 2012; Ebner et al. 2015; Ruffman et al. 2006; 2012; Zebrowitz et al. 2013; Zebrowitz et al. 2017). The results are also in accord with an age-related increase in overconfidence in performance on cognitive tasks in older compared to young adults (Crawford and Stankov 1996). Taken together, this pattern of findings suggests that the older adult demographic may be at particular risk for phishing attempts and constitute an important target for anti-phishing education and decision-supportive interventions in cyberspace.

Different from our expectations, however, we did not observe a main effect of user age on susceptibility as measured in the PHIT task. Rather, we found an age-by-gender interaction on susceptibility. In particular, older women, compared to the other demographic groups, showed the highest susceptibility to phishing. This finding is in line with previous research that showed greater susceptibility to phishing in women than men (Halevi et al. 2015; Sheng et al. 2010). In their study, the gender effect in susceptibility was partially due to the lesser amounts of technical training and technical knowledge of women compared to men. Further, there is evidence of greater computer/Internet usage by young vs. older adults (Morris et al. 2007). Thus, older women may be particularly at risk given their limited experience and knowledge about computers and the Internet. In the present study, we did not specifically inquire about computer literacy and, thus, we cannot speak to this explanation. Future research is warranted to uncover possible contributing factors and delineate underlying mechanisms for this particularly high susceptibility to email phishing in older women (see also Ebner et al. 2018).

Interestingly, when comparing the age groups in their susceptibility over time across the study period, we detected a decrement in the young group's susceptibility to phishing, while the older groups' susceptibility remained stable across the 21 days. This finding is consistent with the literature on economic games, in which older adults have been found to continue to trust their partners even after experiencing a breach of trust from their partners, while young adults adjust their perceptions on their partner's behavior (Suzuki 2016). The continued susceptibility to phishing in older Internet users that we observed across the study duration may indicate an age-related impairment in learning-based adjustment in decision-making (Eppinger et al. 2011; Samanez-Larkin and Knutson 2015) and calls for continued, as opposed to one time, education as well as development of "on-the-spot" phishing detection and warning tools as effective approaches in older adults.

Further qualifying age-group differences in susceptibility to phishing, we observed an age-moderation of the effectiveness of weapons of influence on susceptibility. In particular, while scarcity and authority were more effective in young than older users, reciprocation and liking were more effective in older than young users. These age-group differences in the relative effectiveness of weapons of influence may reflect age-related changes in personal motivations and interests, as suggested by Socioemotional Selectivity Theory (Carstensen et al. 1999; Isaacowitz 2006; Mather and Knight 2005). In particular, this theory proposes that, because of the perceived limitation of future time left in life, older compared to young adults focus more on emotionally meaningful goals. This motivational shift is in line with evidence that loneliness and social isolation are of great concern in older adults, with the potential to result in devastating effects on health and well-being (Shankar et al. 2011). Specifically relevant in the present context, there is evidence that loneliness and negative affect are one of the factors contributing to fraud victimization in the elderly

(Alves and Wilson 2008; Ebner et al. 2018; Lichtenberg et al. 2016). Thus, compared to the other weapons, reciprocation and liking may be particularly effective weapons in phishing of older individuals.

We did not observe age-group differences in the relative effectiveness of life domains on susceptibility. Though health-related information becomes increasingly important in old age (Baltes et al. 1998), phishing emails related to health were not particularly effective in older users. It is possible that because older adults are already inundated with medication advertisements or offers via email (usually seen as spam or annoying advertisement), they might have become desensitized to emails pertaining to these topics. This could explain the low effectiveness of health-related emails in our study. Supporting this possibility, in an independent study we showed that older compared to young Internet users were more likely to receive spam emails referring to health in their everyday lives (Oliveira et al. 2019).

Regarding the relative effectiveness of weapons of influence, overall, scarcity and authority were the two most effective, while commitment and social proof were the two least effective, weapons of influence, in line with previous work in young Internet users (Butavicius et al. 2016). However, in contrast to our findings, the effectiveness of scarcity in this previous study was lower than that of authority and was comparable to that of social proof. Methodological differences between these two studies may explain these discrepancies in results. While the present study measured susceptibility to phishing emails in young and older Internet users via an ecologically valid behavioral design (the PHIT task), Butavicius and colleagues assessed university students' ability to self-report on the safety of links in simulated emails. It is possible that individuals may be able to remind themselves that an opportunity to receive a scarce object at low cost may be a suspicious offer, especially when not personally involved and only presented to them in the form of a scenario; however, when they are unprompted and must decide whether to act on an offer, they may still fall for it, as our data suggest. Consistent with this speculation, participants in the present study showed higher susceptibility awareness to scarcity emails than authority emails, while there was no difference in susceptibility between emails using these two types of weapons in our behavioral paradigm.

Regarding the relative effectiveness of life domains, we observed that legal emails were the most effective for all users. In contrast, somewhat surprisingly, the least effective life domain was financial. This small effectiveness for financial emails may be due to a familiarity effect. In particular, frequent experiences with financial scams in everyday life may have transferred knowledge into the study and could be underlying "resilience" to these types of attacks. Consistent with this speculation, in our independent study of naturally received spam emails by young and older Internet users, financial spam emails were most prevalent while legal spam emails were least prevalent (Oliveira et al. 2019).

Findings from the present study demonstrated that susceptibility to phishing emails varied as a function of the weapons of influence used and the life domains the emails referred to. For example, our finding of high susceptibility for emails using authority and referring to legal matters aligns with work by Halevi et al. (2015) who found very high susceptibility (62%) to simulated phishing emails seemingly sent by the company's IT manager (i.e., an authority) to company employees asking them to download a plug-in per the company's regulations (i.e., a legal matter). In contrast, Benenson et al. (2017) observed a much lower susceptibility (20%) to simulated phishing emails that asked recipients to retrieve party pictures (i.e., liking, social) via clicking on an email-embedded link, in line with our findings that those weapons of influence and life domains are less effective than authority and legal. Thus, our findings invite a novel interpretation of previous findings in light of the importance of email content (specifically the use of weapons of influence and life domains) on susceptibility to phishing.

Many previous research works on susceptibility to phishing was conducted in laboratory settings, possibly affecting the validity of the observation (Hong et al. 2013; Wang et al. 2012). Also, the few existing field experimental approaches were limited to specific contexts, such as the university (Jagatic et al. 2007; Mohebzada et al. 2012) or the company (Halevi et al. 2015) contexts. These contextualized investigations limit the generalizability of the previous findings. In contrast, our study was designed toward broader ecological validity and generalizability by randomly sampling individuals of different ages and gender from a wider population and using a varied set of emails (applying several weapons of influence and a range of life domains).

Also, the small number of simulated phishing emails used in previous studies (i.e., one email per study; Halevi et al. 2015; Jagatic et al. 2007; Mohebzada et al. 2012) did not allow analysis of varying email content on susceptibility. Our study comprised multiple simulated phishing emails with varying content, created based on a large set of authentic spam emails from an independent sample of young and older Internet users (Oliveira et al. 2019). This approach allowed systematic manipulation of some variables (weapons of influence and life domains in the present study) and their consideration in the statistical analysis.

Previous studies showed lower susceptibility in middle-aged than young adults (Halevi et. al. 2015; Sarno et al. 2017; Sheng et al. 2010). This low susceptibility to phishing in middle-aged adults may be related to this group being in the "golden age" of their decision-making, given still relatively intact cognitive ability combined with affluent life experience (Agarwal et al. 2009; Samanez-Larkin 2013). In accord with life-span developmental theory (Baltes 1987), it is, however, also possible that middle-aged adults would show a particular susceptibility to some phishing emails, aligned with the personal goals most relevant in this life phase. For example, previous work found that, compared to young and older adults, middle-aged adults were more likely to become victims of romance scams (Whitty 2015; 2018). Moving forward, it will be interesting to test whether phishing emails using "liking" as the weapon of influence and/or referring to the life domain "social" would be the "Achilles' heel" for middle-aged adults.

It will also be relevant in future research to address the extent to which previous exposure to phishing may affect susceptibility to future attacks among men and women of different ages as well as to determine the extent to which number of phishing emails received on a regular base in real life determines overall susceptibility. Thus, we propose for future work (with adequate privacy and data protection procedures in place) to capture information such as spam email box volume, computer literacy, and Internet usage in the attempt to determine the impact of these factors on susceptibility to email phishing.

7 CONCLUSION

This article reported novel findings regarding susceptibility to phishing as a function of Internet user demographics (age and gender) and email characteristics (use of weapons of influence and life domains to lure users into clicking on email links). The data showed that older women were the most susceptible demographic to phishing. Furthermore, the effectiveness of phishing differed by weapons of influence and life domains and, directly comparing the age groups, young users were most susceptible to scarcity, while older adults were most susceptible to reciprocation. We also observed an intriguing discrepancy between participants' high behavioral susceptibility while low self-reported susceptibility awareness, which was particularly prominent among older users.

Current security training and warning solutions for Internet threats affecting end-users operate under the implicit assumption that *one-size-fits-all*. However, our work suggests that this is not the case. In fact, susceptibility, and therefore the efficiency of phishing, varied by user demographic; with older women particularly vulnerable to the attacks and older compared to

young Internet users little aware of these risks. Susceptibility was also affected by the weapons of influence and life domains applied in the phishing emails, partly in an age-differential fashion. Based on these findings, we propose that security communication and education take user demographics and email content into consideration. Security education and warnings that attempt to accomplish too much and lack personalization (e.g., consider individual variables like age and gender) may not be effective. The novel perspective adopted in our research has promise to benefit the development of the next generation of defense solutions for Internet users, also with an eye toward improving user-friendliness and compliance, with the goal to enhance effectiveness of security measures.

A APPENDICES: DETAILS OF STUDY PROCEDURE

A.1 Terminology and Definitions

Cron Job—Time-based process scheduler in Unix-like operating systems. These processes can be scheduled to perform commands or shell scripts at specific times or intervals.

MySQL—An open-source relational database management system.

Plugin—A software component/extension that adds a specific feature to an existing computer program. Certain software allows for programming "entry points" where developers can interface with features and information of an existing program.

URL—Uniform Resource Locator—A reference to a web resource, colloquially a "web address." A URL is a specific case of URI (Uniform Resource Indicator).

Wordpress—An open-source website content management system that allows for visual editing of website content.

A.2 Server Architecture and Study Framework

For user convenience and to allow broader and more representative participant recruitment, we implemented a browser plugin for various types and versions of popular browsers: Internet Explorer, Chrome, Safari, and Firefox. This plugin tracked all URLs visited by participants during the study period together with access timestamps. As shown in Figure 6(A) below, the plugin continuously sent to the *Log Manager* all URLs visited with their corresponding timestamps. This information was recorded in log files in the *Log Manager*. The plugin did not collect sensitive and personal information from participants, such as bytes transferred in network connections and file accesses, keys typed, or names of files accessed. Participants were identified solely by an ID, which reflected their age group (young, older) and gender (female, male).

Using a controlled timeline and systematic counterbalancing scheme (see Sending Simulated Phishing Emails), as shown in Figure 1(A) below, (1) a set of cron jobs triggered a software module, called Phishing Manager, which (2) retrieved participant and schedule information and simulated phishing emails from the database, and (3) sent simulated phishing emails to the users. The Phishing Manager also recorded presence or absence of study activity, and, as needed, sent reminder emails for Internet activities, and recorded the day of the study.

A Linux machine with Intel Xeon CPU E5-2650 0 2.00GH and 4GB of memory was used to run the server and the study software framework. A MySQL database on the server stored the four sets of simulated phishing emails and participant information for email personalization (e.g., first and last name and county of residence). We used WordPress to deploy and host facade web pages that accompanied the links in the simulated phishing emails. Participant log data occupied 3.04MB in total and 23.38KB per participant on average.

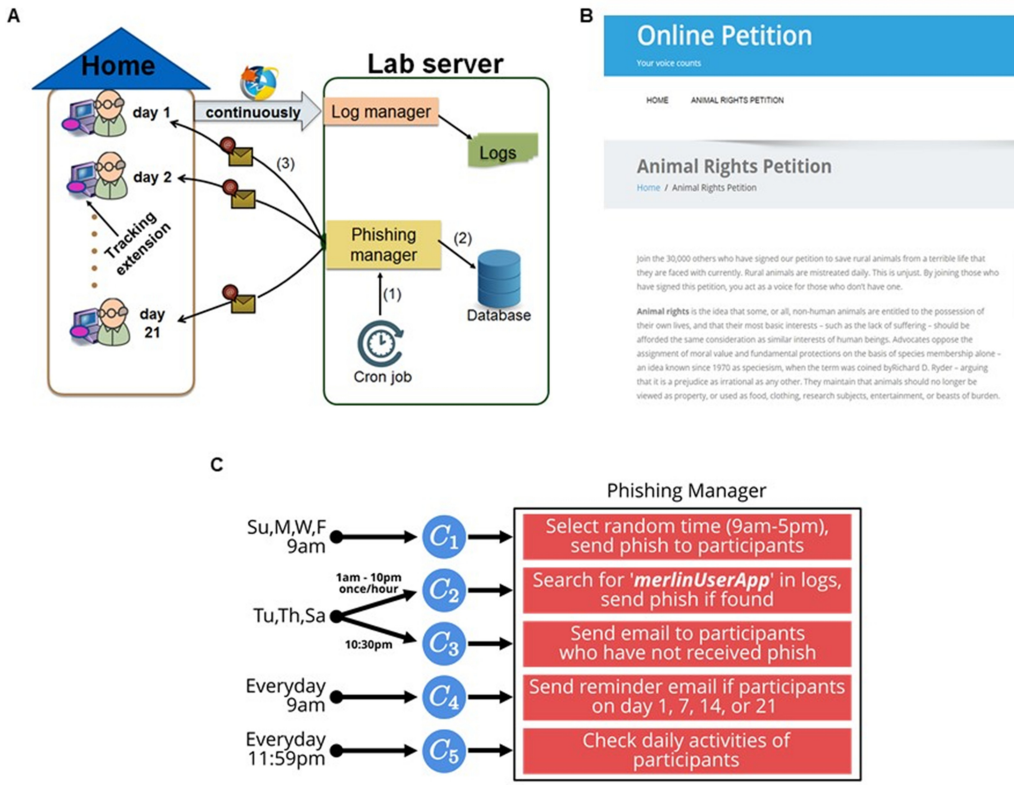

Fig. 6. Phishing Internet Task (PHIT). (A) Overall framework of PHIT. (1) Daily cron jobs invoked the phishing manager to (2) fetch participant, schedule, and spear-phishing emails from the database, and (3) send spear-phishing emails to the participants. (B). Sample facade web-page created for the study to accompany the link embedded in the spear-phishing email. (C) Overview of cron job implementation and triggered events in phishing manager.

A.3 Development of Simulated Phishing Emails and Maintenance of Fake Email Accounts

In the past, there was a propensity for spam and phishing emails to arrive from senders of unknown domains (e.g., @hotfax.com). Recent phishing, however, has become more targeted and sophisticated and leverages established domains, better grammar, spelling, and targeted interests (Fossi et al. 2011). The goal of our study was to examine (i) user susceptibility to and (ii) efficiency of email content of this new generation of phishing. We, therefore, used mainstream email providers for sending of our phishing emails. In particular, we created 22 fake email accounts (11 with common American female names and 11 with common American male names as fictional owners) hosted by Gmail, AOL, and Outlook/Hotmail. To prevent these accounts from being blocked and the study emails from being flagged by the email providers, before the study, each of the accounts were maintained over two months of regular interpersonal communication by our study team. Once the data collection was underway, we continued to create content for these email accounts.

For the development of our simulated phishing emails, we referred to a large set of real-life spam emails that we had collected in a pilot study from an independent sample of young and older Internet users (Oliveira et al. 2019). None of the original emails from this independent study were

used in the present study. Each email had similar word length (between 50 and 150 words) and followed a similar structure. In particular, the emails contained contextual information, such as current events, relevant to the geographical area (e.g., city, county) where this study was located. The emails were personalized, addressing participants by their names, had a unique sender, and contained a link that directed the user to one of 70 facade web pages that we had created for this study (see Figure 6(B) above for an example of a facade web page). All facade web pages were harmless and were hosted on seven web domains purchased for this study.

Each email used one of the seven weapons of influence and one of the six life domains. Three independent research assistants reviewed all emails to assure representation of only one weapon of influence and one life domain per email. In total, we created 84 phishing emails, which covered all possible combinations of weapons of influence and life domains. We evenly separate those 84 emails into four comparable sets (i.e., 21 emails in each set). Each participant was randomly assigned to one of these sets during the three-week study intervention and to another set in the survey on the last study day. This counterbalancing scheme considered age group and gender of the participant. The full set of simulated phishing emails can be retrieved at https://github.com/danielaoliveira/Counter-Balanced-Emails---Weapons-of-Influence-and-Life-Domains.

A.4 The Plugin

We developed a plugin for the four most popular browsers at the time of this study: Chrome, Firefox, Safari, and Internet Explorer. At installation of the plugin, a popup window asked for the participant's age group, gender, and email address. The plugin created a unique ID for each participant based on age group and gender only. The email address was required and used only for the outgoing phishing emails. URL logs were associated only with the unique participant ID. The plugin could not track web activity if the participant was browsing in private mode. Thus, as part of the study enrollment and consent form, we instructed participants not to browse in private mode.

A.5 Sending Simulated Phishing Emails

The Phishing Manager, implemented in Java, was controlled by five cron jobs (C 1–C 5). Figure 6(C) above shows an overview of the cron job implementation. Depending on the day of the week, participants received emails either at a random time of the day, or at a time as close as possible to the time they were engaged in study-related browsing activities.

C 1 ran every Sunday, Monday, Wednesday, and Friday at 9am and invoked the Phishing Manager to randomly select a time between 9am and 5pm to send a personalized phishing email to each active participant based on the counterbalancing scheme. C 2 ran every Tuesday, Thursday, and Saturday and invoked the Phishing Manager to track a participant's web activities and send the personalized phishing email as soon as it detected Internet activity from the participant (see the Procedure in the main text for a description of the scheduled Internet activities participants engaged in as part of the study). C 2 invoked the Phishing Manager every hour from 1am to 10pm to check a participant's Internet activity. At 10:30pm, C 3 invoked the Phishing Manager to send a phishing email to all users who had not yet received a phishing email due to lack of web activity. C 4 ran daily at 9am to invoke the Phishing Manager to send a reminder email if users were on Day 1, 7, 14, or 21 of the study. Finally, C 5 ran each day at 11:59pm invoking the Phishing Manager to generate a participant's activity report. These activity reports did not include any personal identifiable information; they represented a summary of data already present in the log files. Based on these reports, our team contacted participants in a timely manner in case of lapsed study activity. In particular, we contacted participants via phone and email if either their Internet activity or daily

survey was absent for three or more days. All cron jobs code can be retrieved at https://github.com/danielaoliveira/Counter-Balanced-Emails---Weapons-of-Influence-and-Life-Domains.

A.6 References

M. Fossi, G. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, and P. Wood. 2011. Symantec internet security threat report trends for 2010. Volume XVI. Symantec Corporation.

D. S. Oliveira, T. Lin, H. Rocha, D. Ellis, S. Dommaraju, H. Yang, D. Weir, S. Marin, and N. C. Ebner. 2019. Empirical analysis of weapons of influence, life domains, and demographic-targeting in modern spam: An age-comparative perspective. In *Crime Science*. Springer.

ACKNOWLEDGMENTS

We would like to thank Melis Muradoglu, Devon Weir, Paul Talty, Huizi Yang, Adam Soliman, Aliye Karakoyun, Dinia Salmeron, Marvis Cruz, Sebastian Marin, Andrew Varan, Robert Rainer, Cheyenne Reynolds, Hannah Burrichter, Nicole Phillips, Sami Winder, and Andrea Alonzo for their contributions to this project.

REFERENCES

S. Agarwal, J. C. Driscoll, X. Gabaix, and D. Laibson. 2009. The age of reason: Financial decisions over the life cycle and implications for regulation. *Brookings Papers on Economic Activity Fall*, 51–117.

L. M. Alves and S. R. Wilson. 2008. The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of Elder Abuse & Neglect* 20 (2008), 63–85.

P. E. Bailey, T. Ruffman, and P. Rendell. 2013. Age-related differences in social economic decision making: The ultimatum game. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences* 68 (2013), 356–363.

P. E. Bailey, G. Slessor, M. Rieger, P. G. Rendell, A. A. Moustafa, and T. Ruffman. 2015. Trust and trustworthiness in young and older adults. *Psychology and Aging* 30 (2015), 977–986.

P. E. Bailey, P. Szczap, S. N. McLennan, G. Slessor, T. Ruffman, and P. G. Rendell. 2016. Age-related similarities and differences in first impressions of trustworthiness. *Cognition and Emotion* 30 (2016), 1017–1026.

P. B. Baltes. 1987. Theoretical propositions of life-span developmental psychology: On the dynamics between growth and decline. *Developmental Psychology* 26 (1987), 611–626.

P. B. Baltes, U. Lindenberger, and U. M. Staudinger. 1998. Life span theory in developmental psychology. In *Handbook of Child Psychology*. John Wiley & Sons, Inc.

Z. Benenson, F. Gassmann, and R. Landwirth. 2017. Unpacking spear phishing susceptibility. In *International Conference on Financial Cryptography and Data Security*. Springer, Cham, 610–627.

T. Bradley. 2011. Cisco Report-Email Attacks: This Time It's Personal. Retrieved from http://itknowledgeexchange.techtarget.com/security-detail/cisco-report-email-attacks-this-time-its-personal/

J. Brandt, M. Spencer, and M. Folstein. 1988. The telephone interview for cognitive status. Neuropsychiatry, *Neuropsychology, & Behavioral Neurology* 1 (1988), 111–117.

M. Butavicius, K. Parsons, M. Pattinson, and A. McCormac. 2016. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. In *Proceedings of the 26th Australasian Conference on Information Systems, Adelaide, Australia*.

D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson. 2014. Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy* 12 (2014), 28–38.

J. Carr. 2011. *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reily Media, Sebastopol, CA.

L. L. Carstensen, D. M. Isaacowitz, and S. T. Charles. 1999. Taking time seriously: A theory of socioemotional selectivity. *American Psychologist* 54 (1999), 165–181.

L. L. Carstensen and J. A. Mikels. 2005. At the intersection of emotion and cognition: Aging and the positivity effect. *Current Directions in Psychological Science* 14 (2005), 117–121.

E. Castle, N. I. Eisenberger, T. E. Seeman, W. G. Moons, I. A. Boggero, M. S. Grinblatt, and S. E. Taylor. 2012. Neural and behavioral bases of age differences in perceptions of trust. *Proceedings of the National Academy of Sciences* 109 (2012), 20848–20852.

R. B. Cialdini. 2007. *Influence: The psychology of Persuasion*. Collins Business Essentials, New York, NY.

J. D. Crawford and L. Stankov. 1996. Age differences in the realism of confidence judgements: A calibration study using tests of fluid and crystallized intelligence. *Learning and Individual Differences* 8 (1996), 83–103.

N. C. Ebner, P. E. Bailey, M. Horta, J. Joiner, and S. W. C. Chang. 2015. Multidisciplinary perspective on prosociality in aging. In *Frontiers in Developmental Science: Social Cognition Development Across the Life Span*. J. Sommerville and J. Decety (Eds.), Routledge/Taylor & Francis Group, New York, NY, 303–325.

N. C. Ebner, D. M. Ellis, T. Lin, H. A. Rocha, H. Yang, S. Dommaraju, A. Soliman, D. L. Woodard, G. R. Turner, N. Spreng, and D. S. Oliveira. 2018. Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences* (2018).

N. C. Ebner, A. M. Freund, and P. B. Baltes. 2006. Developmental changes in personal goal orientation from young to late adulthood: From striving for gains to maintenance and prevention of losses. *Psychology and Aging* 21 (2006), 664–678.

B. Eppinger, D. Hämmerer, and S. C. Li. 2011. Neuromodulation of reward-based learning and decision making in human aging. *Annals of the New York Academy of Sciences* 1235 (2011), 1–17.

J. S. B. Evans. 2008. Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review of Psychology* 59 (2008), 255–278.

J. S. B. Evans. 2010. Intuition and reasoning: A dual-process perspective. *Psychological Inquiry* 21 (2010), 313–326.

M. Fernandes, M. Ross, M. Wiegand, and E. Schryer. 2008. Are the memories of older adults positively biased? *Psychology and Aging* 23 (2008), 297–306.

A. Ferreira and G. Lenzini. 2015. An analysis of social engineering principles in effective phishing. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST'15)*. IEEE, 9–16.

D. Fisher. 2011. RSA: SecurID Attack Was Phishing Via an Excel Spreadsheet. Retrieved from https://threatpost.com/rsa-securidattack-was-phishing-excelspreadsheet-040111/75099/

I. Fette, N. Sadeh, and A. Tomasic. 2007. Learning to detect phishing emails. In *Proceedings of the 16th International Conference on World Wide Web*. ACM, New York, NY, 649–656.

B. L. Fredrickson and L. L. Carstensen. 1990. Choosing social partners: How old age and anticipated endings make people more selective. *Psychology and Aging* 5 (1990), 335–347.

H. H. Fung, L. L. Carstensen, and F. R. Lang. 2001. Age-related patterns in social networks among European Americans and African Americans: Implications for socioemotional selectivity across the life span. *The International Journal of Aging and Human Development* 52 (2001), 185–206.

K. E. Flynn, M. A. Smith, and J. Freese. 2006. When do older adults turn to the internet for health information? Findings from the Wisconsin longitudinal study. *Journal of General Internal Medicine* 21 (2006), 1295–1301.

V. Garg, L. Lorenzen-Huber, L. J. Camp, and K. Connelly. 2012. Risk communication design for older adults. *Gerontechology* 11 (2012), 166.

B. E. Gavett, R. Zhao, S. E. John, C. A. Bussell, J. R. Roberts, and C. Yue. 2017. Phishing suspiciousness in older and younger adults: The role of executive functioning. *PloS One* 12 (2017), e0171620.

G. Gigerenzer and W. Gaissmaier. 2011. Heuristic decision making. *Annual Review of Psychology* 62 (2011), 451–482.

C. Hadnagy. 2010. *Social Engineering: The Art of Human Hacking*. Wiley Publishing, Inc.

T. Halevi, N. Memon, and O. Nov. 2015. Spear-phishing in the wild: A real-word study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Social Science Research Network*. DOI : http://dx.doi.org/10.2139/ssrn.2544742

R. Helson and V. S. Kwan. 2000. Personality development in adulthood: The broad picture and processes in one longitudinal sample. *Advances in Personality Psychology* 1 (2000), 77–106.

K. W. Hong, C. M. Kelley, R. Tembe, E. Murphy-Hill, and C. B. Mayhorn. 2013. Keeping up with the joneses: Assessing phishing susceptibility in an email task. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. SAGE Publications, Los Angeles, CA, 1012–1016.

J. Hong. 2012. The state of phishing attacks. *Communications of the ACM* 55 (2012), 74–81.

D. M. Isaacowitz. 2006. Motivated gaze: The view from the gazer. *Current Directions in Psychological Science* 15 (2006), 68–72.

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

L. James. 2005. *Phishing Exposed*. Syngress, Canada.

M. Johnson. 1990. Age differences in decision making: A process methodology for examining strategic information processing. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences* 45, 2 (1990), 75–78.

H. S. Jones, J. N. Towse, N. Race, and T. Harrison. 2019. Email fraud: The search for psychological predictors of susceptibility. *PloS One* 14 (2019), e0209684.

D. Kahneman and P. Egan. 2011. *Thinking, Fast and Slow*. Farrar, Straus and Giroux, New York, NY.

P. Kumaraguru, L. F. Cranor, and L. Mather. 2009. Anti-phishing landing page: Turning a 404 into a teachable moment for end users. In *Proceedings of the 6th Conference on Email and Anti-Spam (CEAS'09)*.

P. A. Lichtenberg, M. A. Sugarman, D. Paulson, L. J. Ficker, and A. Rahman-Filipiak. 2016. Psychological and functional vulnerability predicts fraud cases in older adults: Results of a longitudinal study. *Clinical Gerontologist* 39, 1 (2016), 48–63.

R. Mata, A. K. Josef, G. R. Samanez-Larkin, and R. Hertwig. 2011. Age differences in risky choice: A meta-analysis. *Annals of the New York Academy of Sciences* 1235 (2011), 18–29.

M. Mather. 2006. A review of decision-making processes: Weighing the risks and benefits of aging. In *When I'm 64*. L. L. Carastensen and C. R. Hartel (Eds.), National Academies Press, Washington, DC, 145–173.

M. Mather and L. L. Carstensen. 2005. Aging and motivated cognition: The positivity effect in attention and memory. *Trends in Cognitive Sciences* 9 (2005), 496–502.

M. Mather and M. Knight. 2005. Goal-directed memory: The role of cognitive control in older adults' emotional memory. *Psychology and Aging* 20 (2005), 554–570.

J. G. Mohebzada, A. El Zarka, A. H. BHojani, and A. Darwish. 2012. Phishing in a university community: Two large scale phishing experiments. In *Proceedings of the 2012 International Conference on Innovations in Information Technology (IIT'12)*. IEEE, 249–254.

A. Morris, J. Goodman, and H. Brading. 2007. Internet use and non-use: Views of older users. *Universal Access in the Information Society* 6 (2007), 43–57.

National Center for Chronic Disease Prevention and Health Promotion. 2009. *Healthy Aging Improving and Extending Quality of Life Among Older Americans*. Centers for Disease Control and Prevention. Retrieved from http://www.cdc.gov/nccdphp/publications/aag/pdf/healthy_aging.pdf

A. Neupane, K. Satvat, N. Saxena, D. Stavrinos, and H. J. Bishop. 2018. Do social disorders facilitate social engineering? A case study of autism and phishing attacks. In *Proceedings of the 34th Annual Computer Security Applications Conference*. ACM, New York, NY, 467–477.

Netcraft Toolbar 2010. Netcraft, Ltd. Retrieved from http://toolbar.netcraft.com

Y. S. Oh and Y. Cho. 2015. Examining the relationships between resources and online health information seeking among patients with chronic diseases and healthy people. *Social Work in Health Care* 54 (2015), 83–100.

D. S. Oliveira, T. Lin, H. Rocha, D. Ellis, S. Dommaraju, H. Yang, D. Weir, S. Marin, and N. C. Ebner. 2019. Empirical analysis of weapons of influence, life domains, and demographic-targeting in modern spam: An age-comparative perspective. *Crime Science* 8 (2019). DOI: https://doi.org/10.1186/s40163-019-0098-8

T. Pachur, R. S. Suter, and R. Hertwig. 2017. How the twain can meet: Prospect theory and models of heuristics in risky choice. *Cognitive Psychology* 93 (2017), 44–73.

A. Perrin and M. Duggan. 2015. Americans' Internet access: 2000–2015. Retrieved from http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/

R. Peters. 2006. Ageing and the brain. *Postgraduate Medical Journal* 82 (2006), 84–88.

E. Peters, T. M. Hess, D. Västfjäll, and C. Auman. 2007. Adult age differences in dual information processes: Implications for the role of affective and deliberative processes in older adults' decision making. *Perspectives on Psychological Science* 2 (2007), 1–23.

D. M. Pinsker, K. McFarland, and N. A. Pachana. 2010. Exploitation in older adults: Social vulnerability and personal competence factors. *Journal of Applied Gerontology* 29 (2010), 740–761.

A. E. Reed, L. Chan, and J. A. Mikels. 2014. Meta-analysis of the age-related positivity effect: Age differences in preferences for positive over negative information. *Psychology and Aging* 29 (2014), 1–15.

M. Ross, I. Grossmann, and E. Schryer. 2014. Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science* 9, 4 (2014), 427–442.

T. Ruffman, J. Murray, J. Halberstadt, and T. Vater. 2012. Age-related differences in deception. *Psychology and Aging* 27 (2012), 543–549.

T. Ruffman, S. Sullivan, and N. Edge. 2006. Differences in the way older and young adults rate threat in faces but not situations. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences* 61 (2006), 187–194.

G. R. Samanez-Larkin. 2013. Financial decision making and the aging brain. *APS Observer* 26, 5 (2013), 30–33.

G. R. Samanez-Larkin and B. Knutson. 2015. Decision making in the ageing brain: changes in affective and motivational circuits. *Nature Reviews. Neuroscience* 16 (2015), 278–289.

D. M. Sarno, J. E. Lewis, C. J. Bohil, M. K. Shoss, and M. B. Neider. 2017. Who are phishers luring? A demographic analysis of those susceptible to fake emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*.

A. Shankar, A. McMunn, J. Banks, and A. Steptoe. 2011. Loneliness, social isolation, and behavioral and biological health indicators in older adults. *Health Psychology* 30 (2011), 377–385.

J. Shao, W. Du, T. Lin, X. Li, J. Li, and H. Lei. 2019. Credulity rather than general trust may increase vulnerability to fraud in older adults: A moderated mediation model. *Journal of Elder Abuse & Neglect* 31, 2 (2019), 146–162.

S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 373–382.

S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. 2007. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*. ACM, 88–99.

S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong, and C. Zhang. 2009. An empirical analysis of phishing blacklists. In *Proceedings of the 6th Conference on Email and Anti-Spam (CEAS'09)*.

P. W. Singer and A. Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

R. N. Spreng, J. Karlawish, and D. C. Marson. 2016. Cognitive, social, and neural determinants of diminished decision-making and financial exploitation risk in aging and dementia: A review and new model. *Journal of Elder Abuse & Neglect* 28 (2016), 320–344.

L. Sugiura. 2013. To deceive or not to deceive! Legal implications of phishing covert research. *International Journal of Intellectual Property Management* 6 (2013), 285–293.

A. Suzuki. 2016. Persistent reliance on facial appearance among older adults when judging someone's trustworthiness. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences* 73 (2016), 573–583.

K. Tentori, D. Osherson, L. Hasher, and C. May. 2001. Wisdom and aging: irrational preferences in college students but not older adults. *Cognition* 81, 3 (2001), B87–B96.

A. Terracciano, R. R. McCrae, L. J. Brant, and P. T. Costa Jr. 2005. Hierarchical linear modeling analyses of the NEO-PI-R scales in the Baltimore longitudinal study of aging. *Psychology and Aging* 20 (2005), 493–506.

J. C. Tomaszczyk and M. A. Fernandes. 2012. A positivity effect in autobiographical memory, but not phonemic fluency, in older adults. *Aging, Neuropsychology, and Cognition* 19 (2012), 699–722.

P. A. Tun and M. E. Lachman. 2006. Telephone assessment of cognitive function in adulthood: The brief test of adult cognition by telephone. *Age and Ageing* 35 (2006), 629–632.

S. Uebelacker and S. Quiel. 2014. The social engineering personality framework. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST'14)*. IEEE, 24–30.

United States 2010 Census. 2010. Retrieved from https://www.census.gov/programs-surveys/decennial-census/decade.2010.html

P. Verhaeghen and T. A. Salthouse. 1997. Meta-analyses of age-cognition relations in adulthood: Estimates of linear and nonlinear age effects and structural models. *Psychological Bulletin* 122, 3 (1997), 231–249.

T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor, and N. Christin. 2013. QRishing: The susceptibility of smartphone users to QR code phishing attacks. In *Financial Cryptography and Data Security*. Springer, Berlin, 52–69.

J. Wang, T. Herath, R. Chen, A. Vishwanath, and H. R. Rao. 2012. Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication* 55 (2012), 345–362.

D. Watson, L. A. Clark, and A. Tellegen. 1988. Development and validation of brief measures of positive and negative affect: The PANAS scales. *Journal of Personality and Social Psychology* 54 (1988), 1063–1070.

S. J. Westerman and D. R. Davies. 2000. Acquisition and application of new technology skills: The influence of age. *Occupational Medicine* 50 (2000), 478–482.

M. T. Whitty. 2013. The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology* 53 (2013), 665–684.

M. T. Whitty. 2015. Anatomy of the online dating romance scam. *Security Journal* 28 (2015), 443–455.

M. T. Whitty. 2018. Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking* 21 (2018), 105–109.

T. Wrightson. 2014. *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization*. McGraw-Hill Education.

S. A. Wood, P. J. Liu, Y. Hanoch, and S. Estevez-Cores. 2015. Importance of numeracy as a risk factor for elder financial exploitation in a community sample. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences* 71 (2015), 978–986.

L. A. Zebrowitz, J. Boshyan, N. Ward, A. Gutchess, and N. Hadjikhani. 2017. The older adult positivity effect in evaluations of trustworthiness: Emotion regulation or cognitive capacity? *PloS One* 12 (2017), e0169823.

L. A. Zebrowitz, R. G. Franklin Jr, S. Hillman, and H. Boc. 2013. Older and young adults' first impressions from faces: Similar in agreement but different in positivity. *Psychology and Aging* 28 (2013), 202–212.

Y. Zhang, S. Egelman, L. Cranor, and J. Hong. 2007. Phinding phish: Evaluating anti-phishing tools. In *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS'07)*.

Received October 2018; revised April 2019; accepted May 2019