Phishing in an academic community: A study of user susceptibility and behavior

Alejandra Diaz, Alan T. Sherman & Anupam Joshi

Taylor & Francis
Taylor & Francis Group

Check for updates

Phishing in an academic community: A study of user susceptibility and behavior

Alejandra Diaz [iD], Alan T. Sherman [iD], and Anupam Joshi

ABSTRACT

We present an observational study on the relationship between demographic factors and phishing susceptibility at the University of Maryland, Baltimore County (UMBC). In spring 2018, we delivered phishing attacks to 450 randomly selected students on three different days (1,350 students total) to examine user click rates and demographics among UMBC's undergraduates. Participants were initially unaware of the study. We deployed the billing problem, contest winner, and expiration date phishing tactics. Experiment 1 impersonated banking authorities; Experiment 2 enticed users with monetary rewards; and Experiment 3 threatened users with account cancelation. We found correlations resulting in lowered susceptibility based on college affiliation, academic year progression, cyber training, involvement in cyber clubs or cyber scholarship programs, time spent on the computer, and age demographics. We found no significant correlation between gender and susceptibility. Contrary to our expectations, we observed a reverse correlation between phishing awareness and student resistance to clicking. Students who identified themselves as understanding the definition of phishing had a higher susceptibility rate than did their peers who were merely aware of phishing attacks, with both groups having a higher susceptibility rate than those with no knowledge whatsoever. Approximately 70% of survey respondents who opened a phishing email clicked on it, with 60% of student having clicked overall.

Introduction

Typically, the most important and devastating vulnerability a company can have is its very own people (Howarth 2014). The human factor, or error, is responsible for 95% of security incidents (Howarth 2014). Malicious actors aim to use social engineering to exploit users into giving up valuable and confidential information (Norton 2014). We present results from a study of susceptibility of undergraduate students to phishing emails. In *phishing*, a fraudulent entity tries to gain user information, possibly posing as an authority.

This observational study is the first to examine age, gender, college affiliation, academic year progression, time spent on a computer, cyber club/cyber scholarship program affiliation, cyber training, and phishing awareness demographics in one study. Our motivation lies in understanding dependent variables in a student population for future training tailored to individual students. We hope our results will help businesses and colleges improve their cybersecurity practices.

As summarized in the tables and figures, our contributions are the results and analyses from our observational study in which we sent phishing emails to 1,350 University of Maryland, Baltimore County (UMBC) students. For more details, see Diaz (2018).

Previous work

There have been few phishing and general cybersecurity related surveys conducted on college students in the past, focusing on the correlation between susceptibility and one or few demographics.

Farooq et al. (2015) studied 1,280 participants in six different colleges throughout India, Malaysia, Nepal, Pakistan, and Thailand. They documented Internet use and its correlation to the student user susceptibility level. A year prior, Farooq et al. (2016) also surveyed 614 university students from eight different majors to calculate their information security awareness score (ISA). They concluded that gender provides an insight on how a student learns cybersecurity skills. Men tend to gain security knowledge through self-taught means, while women tend to prefer formal training and interacting in their social circles (Farooq et al. 2015).

In Tamil Nadu, India, Senthilkumar and Easwaramoorthy (2017) surveyed student responses to cyber themes, such as "virus[es], phishing, fake advertisement, popup windows and other attacks in the internet". In this study, only 10 of the 379 students stated that they would report any malicious activity to their cyber crime office. Similarly, Kim (2013) surveyed a group of undergraduate business students on their knowledge of cyber-related topics. While the students were somewhat knowledgeable on most topics covered in NIST Standard 800-50, Kim (2013) suggested training programs for all students within the college to increase student awareness. Duggan (2008) conducted a comparable survey in Japan, where he surveyed a group of Japanese college students about their cybersecurity and privacy-risk knowledge based on terminology.

Dodge, Carver, and Ferguson (2007) conducted an unannounced phishing test on students at the United States Military Academy to evaluate their cyber training programs. They concluded that the more educated a student was in academic year, the less likely they were to fall for the phishing

scam. Similarly, Aloul (2012) presented a project in which a fake website portal recorded the number of students who navigate to this phishing trap. They recorded 9% of the 11,000 students falling for the fraudulent portal.

Sheng et al. (2010) studied if age, sex, and education level influenced phishing susceptibility. They determined that higher education level, age, and being male lead to less susceptibility. Sun et al. (2016) investigated links between gender and behavior. In contrast, the research team did not find a significant difference in gender. In these two studies, the users knew that they were being tested on their ability to detect phishing attacks.

In our study, we include a more expansive list of demographics than those explored in previous studies. We also focus on phishing susceptibility rather than on general cybersecurity topics, and we do not inform the participants beforehand of the phishing experiments.

Experimental methodology

We deploy three phishing experiments on randomly selected students at UMBC. To simulate errors commonly found in phishing attempts, these phishing emails contain errors that provide clues of their illegitimacy. Subsequently, we sent a debriefing statement to all selected students, as required by our UMBC Institutional Review Board (IRB) approval. We also sent a survey to gather more demographic data on those students who had opened a phishing email.

Subject population

Our study takes the 11,234 undergraduate students currently enrolled at UMBC as the target pool (UMBC Admissions 2018). UMBC is especially well known for science and technology. UMBC includes three colleges: the College of Arts, Humanities, and Social Sciences, the College of Engineering and Information Technology, and the College of Natural and Mathematical Sciences. Our study focuses on the student's primary major, regardless of any subsequent major, minor, or certificate program (UMBC Admissions 2018).

We sent each phishing email to a randomly selected set of 1,350 students. Each set comprised 450 students, with 150 students from each college.

We decreased the number of eligible students from 11,234 to 10,920, marking students ineligible if they had an undecided major or if they were part of the interdisciplinary studies track. Interdisciplinary studies majors have multiple majors in potentially different colleges.

Experiment 1: PayPal

Experiment 1 deployed the popular *Billing Problem* tactic (Downs, Holbrook, and Cranor 2006). The fraudulent entity claims to be PayPal, a

Processed - Order of Atomic Empire Designs

PayPal <paypalcustomernotifications@gmail.com> ▇▇▇ ↩ ▾
to ▇▇▇▇▇▇▇▇

April 4, 2018 20:06:08 EST
Transaction ID: 06DG3630032N423N

Thank you for your order!

You sent an order of $27.22 USD to Atomic Empire Designs.
Order Details

It may take a few moments for this transaction to appear in your account.

Merchant
Atomic Empire Designs
support@ scifigenredesigns. com
909-5190-7200

Instructions to merchant
You haven't entered any instructions.

Shipping address - confirmed
UMBC
1000 Hilltop Circle
Baltimore, MD 21769
United States

Shipping details
The seller hasn't provided any shipping
details yet.

Description	Unit price	Qty	Amount
Atomic Empire Designs Order #251543	$27.22 USD	1	$27.22 USD
	Subtotal		$27.22 USD
	Tax & shipping		$5.99 USD
	Total owed		$47.22 USD

Copyright © 1929-2019 PayPal, Inc. All rights reserved.
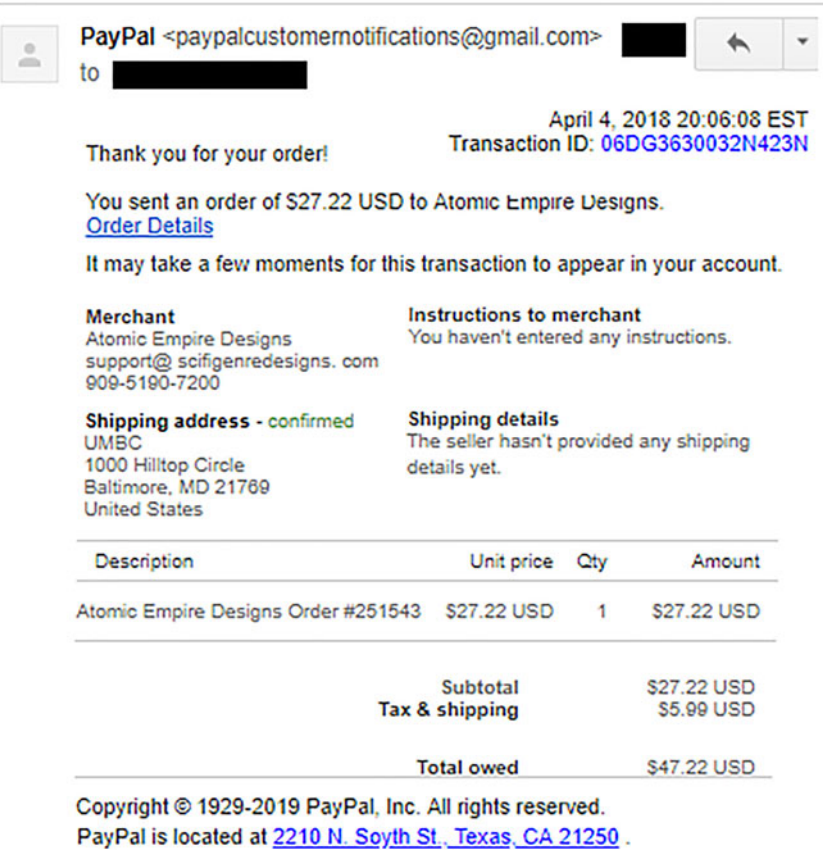PayPal is located at 2210 N. Soyth St., Texas, CA 21250 .

Figure 1. Experiment 1 PayPal email claims to bill the student's PayPal account.

popular online payment company. The email tries to entice the user to click on the email link by claiming to have received an order from them and therefore billing their PayPal account.

There are several red flags that indicate this email is illegitimate. Atomic Empire Designs is a fake company with invalid customer service email and phone number. The shipping address is vague, and the zipcode is incorrect for the Baltimore region. The email timestamp is for a future time, and the total amount of money owed does not add up to the subtotal, plus tax and shipping expenses. The last line of the email stating that "Paypal is located at ... " lists an incorrect and invalid address. Another flag is the sender's email address: any email from the PayPal business will have a "@paypal.com" address, not "gmail.com." The link described as order details is also suspicious. If one hovers over the link, it does not indicate any association with PayPal; instead, it goes through a tracking url that contains a "thisisnotmalware" string (Figure 1).

Experiment 2: Quadmania

In this experiment, we make use of UMBC's Quadmania event, the university's major spring weekend festival, to lure the user through monetary gain (Ellis 2014). The email congratulates the student on their $100 Amazon prize and asks them to click the provided link. This email adds legitimacy by using the 2018 Quadmania banner while the signature of the email proclaims it was sent by the UMBC Events Board. This name is similar to the Student Events Board (SEB) that organizes Quadmania. Futhermore, the email describes a UMCP survey. Not only was no such survey conducted, UMCP refers to the University of Maryland, College Park, which is a different school. There are grammar and spelling inconsistencies, including the keynote singer 21 Savage. When hovering over the link, the user can see the link redirects them to cnn.com after going through a tracking software. The email is sent from a "@umbcalerts.com" address, instead of a "umbc.edu" address (Figure 2).

Experiment 3: DoIT

This email is a variation of the *expiration date* tactic, mimicking UMBC's Division of Information Technology (DoIT). It claims that the user must verify their credentials to keep their UMBC account, referencing the Quadmania phish to add validity. The email threatens that the user must click and verify their identity within 48 hours.

There are several spelling and grammar errors, which are uncommon for official UMBC communications. The authority names itself "Department of Institutional Technology" and later signs off with "UNCP DoIT". There is no Department of Institutional Technology nor UNCP entity at UMBC. The odd quote at the end of the email is out of character and unconventional for a university's IT department. The email address and link of this email are suspicious as well. The user can hover over the link and see that it goes to the Google homepage after going through tracking software. The email address has a "@umbcdoit.com" email address instead of a "@umbc.edu" one (Figure 3).

Debriefing statement and demographic survey

Part of our IRB protocol requires us to send a debriefing email that informs all 1,350 selected students of the study. It also assures that we anonymized all data, kept all data confidential, and could not identify any individual.

We then invited students who were part of the 1,350 target group and opened a phishing email from experiments 1–3 to also participate in a survey. After asking for consent and ensuring the survey respondents were at
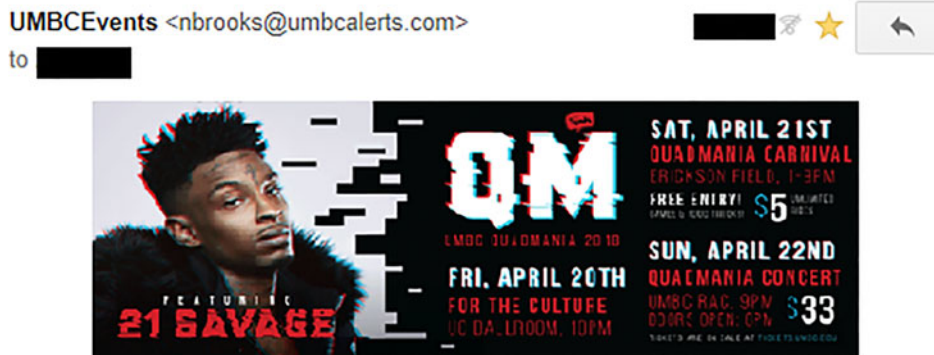
Figure 2. Experiment 2 Quadmania email offers a free $100 gift certificate.

least 18 years of age, we asked questions on their academic year, major affiliation, gender, age, past cybersecurity training, participation in cyber clubs or cyber scholarship programs, phishing awareness, and time spent per day on the computer. We gave a brief definition of phishing and quick tips on how to identify phishing emails. We directed the users to the official UMBC phishing and spam FAQ page for more information.

Data collection

To track the data, we used the free application MailTracker by Hunter and the EmailTracker by cloudHQ (CloudHQ 2018; Hunter 2018). Each of these programs tracked if an email recipient opened an email and whether they clicked any links. Both verify and confirm each other's recorded data.

> **UMBCDoIT** <adam@umbcdoit.com>
> to
>
> [Verification Notice #QRX1497373RT]
>
> Dear student,
> It has come to our attention that there has been a recent "phishing" scheme sent out to several members of our UMBC community over Quadmania event.
>
> As such, UMBC's Department of Institutional Technology (DoIT) is having every possible target of this attack re-verify their identity to ensure our networks are safe. To avoid any network lagging, we have broken down the UMBC community into several groups, where your in group #1.
>
> If you are receiving this message, please be aware that you are **required** to verify your identity in our private servers within 48 hrs. You will be locked out of your UMBC accounts, (including Blackboard, myUMBC, and any Gmail priveledges) unless you update your information in the link provided.
>
> Enable account credentials
>
> You are given a grace period of **24 hours from email receipt date** to complete this action. **Failure to do so will result in account suspension and eventual deletion.**
>
> For any question or concerns, please contact admin@umbcdoit.com.
>
> UNCP DoIT
>
> *"New technology is not good or evil in and of itself. It's all about how people choose to use it."*

Figure 3. Experiment 3 DoIT email threatens to suspend the student's computer account.

Statistical methods

We applied Fisher's exact test and Pearson's chi-square for significance testing, and Cramer's V to test strength of that significance, with $\alpha = 0.05$ (McDonald 2014). We used Fisher's exact test in lieu of the chi-square test when an expected value is less than 5. We defined the null hypothesis as there is no dependency between the demographic factor and student click rate. We used IBM's SPSS to create contingency tables and calculate these statistics.

Results

Of the 1,350 students randomly selected for this study, 1,246 (92%) opened a phishing email in at least one of the three experiments. We sent the debriefing statement to all 1,350 students, and the demographic survey only to those 1,246 students who opened a phishing email. All demographics except for college affiliation were tested with survey respondent data only (Figure 4).
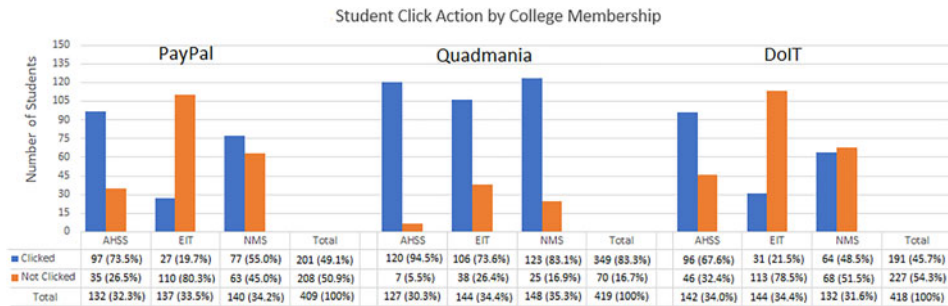
Student Click Action by College Membership

	PayPal				Quadmania				DoIT			
	AHSS	EIT	NMS	Total	AHSS	EIT	NMS	Total	AHSS	EIT	NMS	Total
Clicked	97 (73.5%)	27 (19.7%)	77 (55.0%)	201 (49.1%)	120 (94.5%)	106 (73.6%)	123 (83.1%)	349 (83.3%)	96 (67.6%)	31 (21.5%)	64 (48.5%)	191 (45.7%)
Not Clicked	35 (26.5%)	110 (80.3%)	63 (45.0%)	208 (50.9%)	7 (5.5%)	38 (26.4%)	25 (16.9%)	70 (16.7%)	46 (32.4%)	113 (78.5%)	68 (51.5%)	227 (54.3%)
Total	132 (32.3%)	137 (33.5%)	140 (34.2%)	409 (100%)	127 (30.3%)	144 (34.4%)	148 (35.3%)	419 (100%)	142 (34.0%)	144 (34.4%)	132 (31.6%)	418 (100%)

Figure 4. Number of clicks on phishing emails by students in the College of Arts, Humanities, and Social Sciences (AHSS), the College of Engineering and Information Technology (EIT), and the College of Natural and Mathematical Sciences (NMS).

Experiment 1 results

Of the 450 students receiving the PayPal phishing email, 409 (91%) opened the email. Of those 409 students, a majority of the Arts, Humanities, and Social Sciences majors clicked the link.

We sent emails to 150 students within each college and analyzed the actions of those who opened the email. Seventy-four percent of students in Arts, Humanities, and Social Sciences majors had clicked the link, with 20% in Engineering and Information Technology and 55% in Natural and Mathematical Sciences.

Experiment 2 results

We sent the Quadmania phishing email to 450 students, of which 419 (93%) opened the email. Three hundred forty-nine students (83.3%) clicked the link within the email. Almost all of the Arts, Humanities, and Social Sciences majors clicked the link (95%), often within minutes of receiving the email. Seventy-four percent of students in the College of Engineering and Information Technology clicked the link, while 83% in the College of Natural and Mathematical Sciences clicked.

Experiment 3 results

Ninety-three percent of students opened the third email. Sixty-eight percent of students in the Arts, Humanities, and 49% Social Sciences and Natural and Mathematical Sciences were fooled into clicking the link. In contrast, only 31 students (22%) in Engineering and Information Technology majors clicked.

Survey results

Of the 1,246 students who had the option to complete the survey, 482 students (39%) responded within a 7-day period. For each cohort, at least 100 subjects completed the survey. Figure 4 shows the click action by college membership for each experiment.

Analysis

We analyzed all experiments and survey results and find significant correlations in all tested demographics except gender.

Shown in Table 1 are the percentages of students who have opened the emails and have either clicked or not clicked a link. Included are the percentages of students who have opened an email but have also completed the demographics survey used for the demographics analysis portion.

While around 59–60% of all overall students have clicked a link in an email, there were fluctuations between the three different experiments. In contrast, survey respondents clicked 70% of the time, with fluctuations occurring as well.

Experiments

We found a correlation between college affiliation and user click action. For all three experiments, the chi-square value exceeded 5.991. The aggregate data also had a chi-square value exceeding the critical value, rejecting the null hypothesis. We define the null hypothesis as there being no correlation between user susceptibility and a demographic. A low-to-medium strength of association is also present (Figure 5).

Table 1. Summary of experimental results. Number of students who clicked on phishing emails, among students who were sent emails, opened the emails, and answered the survey.

Action	PayPal	Quadmania	DoIT	Total
Sent emails	450	450	450	**1,350**
Clicked	201 (45%)	349 (78%)	191 (42%)	**741 (55%)**
(% from subjects who were sent emails)				
Did not click	208 (46%)	70 (16%)	227 (50%)	**505 (37%)**
(% from subjects who were sent emails)				
Opened emails	409 (91%)	419 (93%)	418 (93%)	**1,246 (92%)**
(% from subjects who were sent emails)				
Clicked	201 (49%)	349 (83%)	191 (46%)	**41 (59%)**
(% from subjects who opened email)				
Did not click	208 (51%)	70 (17%)	227 (54%)	**505 (41%)**
(% from subjects who opened email)				
Answered survey (% from overall survey respondents)	102 (21%)	225 (47%)	155 (32%)	**482 (100%)**
Clicked	47 (46%)	176 (78%)	116 (75%)	**339 (70%)**
(% from subjects who answered survey)				
Did not click	55 (54%)	49 (22%)	39 (25%)	**143 (30%)**
(% from subjects who answered survey)				

Comparative analysis

We show that phishing awareness, hours spent on the computer, cyber training, cyber club or cyber scholarship affiliation, age, academic year, and college affiliation are significant variables to student susceptibility (Tables 2 and 3).
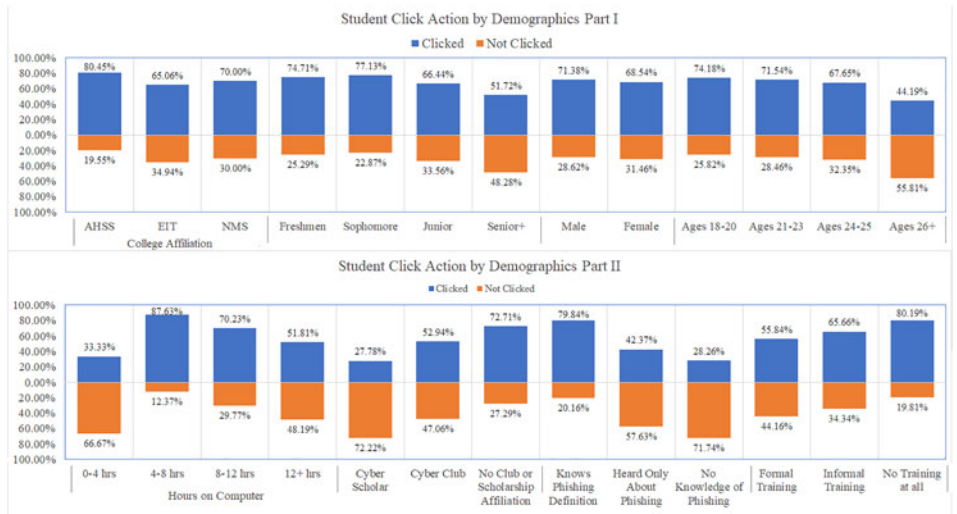

Figure 5. Click action by demographic factors for students who opened email and returned the demographic survey form.

Table 2. Significance of three statistical tests at separating students who click on emails, computed separately for each phishing email, at confidence level α=0.05, with given degrees of freedom (df).

Demographic		Strength of significance Cramer' s V	Significance				Critical value α = 0.05	df
			Fisher's *p* value	Chi-square (χ^2)	χ^2 *p* value			
Significant	PayPal	0.44	<0.0001	80.71	<0.0001		5.991	2
	Quadmania	0.23	<0.0001	21.14	<0.0001		5991	2
	DoIT	0.38	0.0001	61.78	<0.0001		5.991	2
	Aggregate	0.33	0.0001	136.35	<0.0001		5.991	2

Table 3. Significance of three statistical tests at separating students who clicked on a phishing email, by demographic factors, at confidence level α = 0.05, with given degrees of freedom (df).

	Demographic	Strength of significance Cramer's V	Significance				Critical value α = 0.05	df
			Fisher's *p* value	Chi-Square (χ^2)	χ^2 *p* value			
Significant	Phishing awareness	0.40	<0.0001	77.46	<0.0001		5.991	2
	Hours spent on computer	–	<0.0001	–	–		7.815	3
	Cyber training	0.20	0.0001	19.47	<0.0001		5.991	2
	Cyber club or cyber scholarship	0.20	0.0001	19.29	<0.0001		5.991	2
	Age	0.18	0.0017	16.25	0.001		7.815	3
	Academic year	0.18	0.0017	15.67	0.0013		7.815	3
	College affiliation	0.14	0.0068	9.85	0.0073		5.991	2
Insignificant	Gender	–	0.536	043	0.512		3.841	1

The aggregated college affiliation demographic indicates that STEM majors–with Engineering and IT majors in particular–had lower click rates (EIT 65%, NMS 70%) compared with non-STEM majors (AHSS 80%). Increasing academic year progression saw a decrease in student click rate. We observed that increased time on the computer and cyber training correlated with lower click rates. Students in a cyber club or cyber scholarship program also clicked the phishing link less often than did students with no such affiliation. Within the cyber club and cyber scholarship group, students who were affiliated with a cyber scholarship program had lower click rates compared with the cyber club students.

Contrary to our expectations, in experiments 1–3, students who were unaware of phishing attacks performed better (28% clicked) than did students who were aware (42% clicked) or who understood what phishing attacks are (80% clicked).

We found no significant correlation between gender and susceptibility, with the chi-square calculation less than the critical value.

Discussion

We describe the campus response to our phishing emails, discuss an unexpected finding, comment on the nature of the phishing emails, identify study limitations, and present open problems.

Campus response

Although the PayPal email received little attention, the Quadmania phish (purportedly from SEB) created notable confusion. SEB, DoIT, and campus police issued alerts. A few hours after we sent the emails, SEB posted warnings to the student body of a phishing scheme, informing users that they did not send the Quadmania email, spreading word on the *myUMBC* dashboard and social media.

SEB's quick and efficient communication reached several students within the experiment 2 cohort. Despite these warnings, the vast majority of students had already fallen for the Quadmania scheme. Many students who were deceived by the phish reported their experiences to DoIT or SEB, prompting quick responses by SEB and DoIT to us and the student body. While we had notified DoIT in advance, not all of their staff knew about our experiment and, in hindsight, we probably should have also informed SEB in advance.

An unexpected finding

As expected, we observed lower user susceptibility with college affiliation, academic year, age, cyber club and cyber scholarship affiliation, amount of

time spent on the computer, and cyber training. Contrary to our expectations, we observed greater user susceptibility with greater phishing knowledge and awareness.

We have no convincing explanation for this finding, and we do not know if it is reproducible. Nevertheless, we consider two speculations. First, it is possible that the act of falling for the phishing scheme might have increased the user's awareness about phishing. In hindsight, it might have been wiser to have asked in the post-event survey what was the level of phishing awareness the user had when they opened the phishing email. Second, it is conceivable that users who fell for the phish might be more likely to overestimate their knowledge, including about phishing.

Limitations

Limitations of the study include student awareness of the experiment and veracity of survey responses. Especially given the commotion created by the Quadmania phish, it is possible that there was greater awareness among subjects about the possibility of phishing attacks in the third experiment than in the first two. We made no attempt to measure how accurately and honestly subjects filled out their demographic surveys.

Nature of phishing emails

As explained in Section III, we intentionally inserted many clues into each phishing email of their illegitimacy (e.g., spelling errors) and, initially, we did not inform the subjects about the experiments. Our rationale was to simulate commonly occurring phishing attacks, which often contain such clues. We do not know how much, if at all, such clues affected user behavior. Similarly, we do not know how much, if at all, lack of awareness of the experiment affected user behavior. Given the high click rates, we speculate that, for many users, such clues were not a decisive factor. Similarly, given that study awareness appears to be a more subtle issue and that many users are generally aware about the possibility of phishing attacks, we speculate that lack of awareness of the study did not make a significant difference.

Alarmingly, given the high click rates for our phishing emails with many clues, we believe that most users would be even more highly susceptible to more sophisticated attacks. In a more sophisticated attack, the adversary might surveil the target and construct a compelling customized spear-phishing email free of any obvious clues.

Open problems

It would be interesting to understand our unexpected finding that students who reported greater phishing knowledge were more susceptible.

Additional studies could explore this question and determine if our findings are reproducible. It would be useful to understand how clues and study awareness affect user behavior. It would be interesting to include faculty and staff in a study and to analyze user behaviors over several semesters. More difficult open problems are to explore causal factors in user behaviors and to devise effective ways to combat the threat of phishing attacks, including better user education, email filtering, and system design.

Conclusion

Our study finds an association between several demographic factors and a student's susceptibility to phishing attacks. We observed lower susceptibility for college affiliation, academic year progression, cyber training, involvement in cyber clubs or cyber scholarship programs, amount of time spent on the computer, and age demographics. Surprisingly, despite a lower susceptibility for cyber education or IT expertise, we observed greater susceptibility for phishing awareness. We found no significant correlation for gender.

Phishing attacks are a dangerous form of social engineering that target users every day. Our study shows that user susceptibility to phishing remains a prevalent problem, even among technology-savvy students: nearly 70% of the subjects clicked the phishing link. Our observational study uncovers relationships between demographic factors and susceptibility to phishing. We hope that these findings will be helpful in designing more secure systems and developing more effective cybersecurity training for users.

About the authors

Alejandra Diaz is a cyber software engineer and analyst at Northrop Grumman's Cyber Security Operations Center (CSOC) and an adjunct instructor of computer science at the University of Maryland, Baltimore County (UMBC) in the CSEE Department. She is an active member of the Society of Women Engineers (SWE). Diaz graduated with her Master's degree in computer science with a concentration in cybersecurity in 2018 under the guidance of Alan T. Sherman and Anupam Joshi, and her Bachelor's degree in computer science in 2017 at UMBC. She is a Computing Research Association's (CRA) Scholarship for Women Studying Information Security (SWSIS) scholar, a Center of Women in Technology (CWIT) Cyber scholar, Honors College scholar, and Phi Kappa Phi Honor Society alumni. Her research interests include botnet detection and social engineering.

Alan T. Sherman is a Professor of computer science at the University of Maryland, Baltimore County (UMBC) in the CSEE Department and Director

of UMBC's Center for Information Security and Assurance (CISA). His main research interest is high-integrity voting systems. He has carried out research in election systems, algorithm design, cryptanalysis, theoretical foundations for cryptography, applications of cryptography, and cybersecurity education. Sherman is also a private consultant performing security analyses. Sherman earned the Ph.D. degree in computer science at MIT in 1987 studying under Ronald L. Rivest. www.csee.umbc.edu/~sherman

Anupam Joshi is the Oros Family Professor and Chair of Computer Science and Electrical Engineering Department at the University of Maryland, Baltimore County (UMBC). He is the Director of UMBC's Center for Cybersecurity, and one of the USM leads for the National Cybersecurity FFRDC. He is a Fellow of IEEE. Dr. Joshi obtained a B.Tech degree from IIT Delhi in 1989, and a Masters and Ph.D. from Purdue University in 1991 and 1993 respectively. His research interests are in the broad area of networked computing and intelligent systems. His primary focus has been on data management and security/privacy in mobile/pervasive computing environments, and policy driven approaches to security and privacy. He is also interested in Semantic Web and Data/Text/Web Analytics, especially their applications to (cyber) security. He has published over 250 technical papers with an h-index of 79 and over 23,250 citations (per Google scholar), filed and been granted several patents, and has obtained research support from National Science Foundation (NSF), NASA, Defense Advanced Research Projects Agency (DARPA), U.S. Dept of Defense (DoD), NIST, IBM, Microsoft, Qualcom, Northrop Grumman, and Lockheed Martin amongst others.

ORCID

Alejandra Diaz ⬛ http://orcid.org/0000-0002-7563-4214
Alan T. Sherman ⬛ http://orcid.org/0000-0003-1130-4678

References

Aloul, F. A. 2012. The need for effective information security awareness. *Journal of Advances in Information Technology* 3:176–83.

CloudHQ. 2018. EmailTracker. https://www.cloudhq.net/.

Diaz, A. 2018. Phishing in an academic community: A study of user susceptibility and behavior. M.S. thesis, Computer Science and Electrical Engineering Department, University of Maryland, Baltimore County.

Dodge, R. C., C. Carver, and A. J. Ferguson. 2007. Phishing for user security awareness. *Computers and Security* 26 (1):73–80. doi:10.1016/j.cose.2006.10.009.

Downs, J. S., M. B. Holbrook, and L. F. Cranor. 2006. *Decision strategies and susceptibility to phishing*. Carnegie Mellon University.

Duggan, J. 2008. A survey of internet-based risk awareness among Japanese college students. In *Proceedings of E-Learn 2008–world conference on E-Learning in corporate, government, healthcare, and higher education*, ed. C. Bonk, M. Lee and T. Reynolds, 2158–63. Las Vegas, NV: Association for the Advancement of Computing in Education (AACE).

Ellis, D. 2014. Top 10 types of phishing emails. SecurityMetrics Blog. SecurityMetrics blog. securitymetrics.com/2014/05/types-of-phishing-emails.html.

Farooq, A., J. Isoaho, S. Virtanen, and J. Isoaho. 2015. Observations on genderwise differences among university students in information security awareness. *International Journal of Information Security and Privacy* 9 (2):60–74. doi:10.4018/IJISP.2015040104.

Farooq, A., et al. 2016. Dimensions of Internet use and threat sensitivity: An exploratory study among students of higher education. 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), 534–41.

Howarth, F. 2014. The role of human error in successful security attacks. Security Intelligence. https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/.

Hunter. 2018. MailTracker. https://hunter.io/.

Kim, E. B. 2013. Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective* 22 (4):171–9. doi:10.1080/19393555.2013.828803.

McDonald, J. H. 2014. *Handbook of biological statistics*. 3rd ed. www.biostathandbook.com/index.html.

Norton. 2014. What is social engineering? Symantec. https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html.

Senthilkumar, K. and S. Easwaramoorthy. 2017. A survey on cyber security awareness among college students in Tamil Nadu. IOP Conference Series Materials Science and Engineering, Vol. 263.

Sheng, S., M. B. Lanyon, P. Kumaraguru, L. Cranor, and J. Downs. 2010. *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*. Carnegie Mellon University.

Sun, J. C.-Y., S.-J. Yu, S. S. J. Lin, and S.-S. Tseng. 2016. The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior* 59:249–57. doi:10.1016/j.chb.2016.02.004.

UMBC Admissions. 2018. Student enrollment and persistence. UMBC. https://umbc.app.box.com/s/1torn5ywqscyktvo48xnqdlin1rdhf2k.