ILLINOIS
Office for the Protection
of Research Subjects

IORG0000014 • FWA #00008584

Notice of Approval: New Submission

March 19, 2018

Principal Investigator	Michael Bailey
CC	Zane Ma; Joshua Reynolds; Joseph Dickinson; Joshua Mason
Protocol Title	The Impact of Security Protocols on Phishing Efficacy
Protocol Number	18554
Funding Source	National Science Foundation
Review Type	Expedited 7
Status	Active
Risk Determination	No more than minimal risk
Approval Date	03/19/2018
Expiration Date	03/18/2019

This letter authorizes the use of human subjects in the above protocol. The University of Illinois at Urbana-Champaign Institutional Review Board (IRB) has reviewed and approved the research study as described.

The Principal Investigator of this study is reponsible for:

- Conducting research in a manner consistent with the requirements of the University and federal regulations found at 45 CFR 46.
- Requesting approval from the IRB prior to implementing modifications.
- Notifying OPRS of any problems involving human subjects, including unanticipated events, participant complaints, or protocol deviations.
- Notifying OPRS of the completion of the study.

Office for the Protection of Research Subjects
University of Illinois at Urbana-Champaign
(217) 333-2670
irb@illinois.edu

NEW PROTOCOL APPLICATION

Application for Review of Research Involving Human Subjects

This Section is for Office Use Only University of Illinois IRB Protocol No. 18554	Track:
Exempt under 45 CFR §46.101(b) ☐(1) ☐(2) ☐(3) ☐(4) ☐(5) ☐ (6)	Reviewer 1:
Expedite, Category ☐(1)☐(2)☐(3)☐(4)☐(5)☐(6)☐(7)☐(8)☐(9)	Reviewer 2:

All forms must be completed, signed by the RPI, and submitted via email to irb@illinois.edu.

☐ Initial Submission, date of submission _____

☒ Revised New Protocol Application, date of revised New Protocol Application 03/15/2018

1. RESPONSIBLE PROJECT INVESTIGATOR (RPI) The RPI must be a nonvisiting member of the University of Illinois faculty or staff who will serve as project supervisor at Illinois. **For other research team members [including those from other institutions], please complete the Research Team Attachment and provide with the completed application.** Include all persons who will be 1) directly responsible for the project's design or implementation, 2) recruitment, 3) obtain informed consent, 4) involved in data collection, data analysis, or follow-up.

Last Name: Bailey	First Name: Michael		Academic Degree(s): Ph.D.
Dept. or Unit: ECE	Office Address: Room 406		Mail Code:
Street Address: 1308 W. Main Street	City: Urbana	State: IL	Zip Code: 61801
Phone: 217-244-8830	**Fax:**	E-mail: mdbailey@illinois.edu	
Urbana-Champaign Campus Status: Nonvisiting member of (Mark One) **[X] Faculty [ ] Academic Professional/Staff**			
Training ☒ **CITI Training, Date of Completion, 02/16/2018** ☐ **Additional training, Date of Completion[1],**			

2. PROJECT TITLE

The Impact of Security Protocols on Phishing Efficacy

3. FUNDING Indicate whether this research is funded by, or application has been made for, a grant, contract, or gift.

[1] Additional CITI modules may be required depending on subject populations or types of research. These include: (i) research enrolling children; (ii) research enrolling prisoners; (iii) FDA regulated research; (iv) data collected via the internet; (v) research conducted in public elementary/secondary schools; and, (vi) researchers conducted in international sites

3A. STATUS ☐ Research is **not funded** and is **not pending** a funding decision (Proceed to Part 4).
☒ Research is **funded** (funding decision has been made).
☐ Funding decision is **pending**. Funding proposal submission date: ☐

3B. SOURCE(S) If the research is funded or pending a funding decision, mark and name all sources:

Type of Funding—check all that apply		Name of Source
☐	**University of Illinois Department, College, or Campus** (includes Research Board and Campus Fellowship Training Grants)	
☒	**Federal** (from federal agencies, offices, departments, centers)	**NSF**
☐	**Commercial Sponsorship & Industry**[23] (from corporations, partnerships, proprietorships)	
☐	**State of Illinois Department or Agency** (from any state office or entity)	
☐	**Gift or Foundation (including UIF)** (public or private foundations, not-for-profit corporations, private gifts)	

→ Check here if the funding is through a Training Grant: ☐

3C. PROPOSAL Attach a complete copy of the funding proposal or contract. ☒ Attached

Sponsor-assigned grant number, if known: **CNS-1505790**

Title of Funding Proposal or Contract, if different from Project Title in Part 2:

TWC SBE: TTP Option: Medium: Collaborative: EPICA: Empowering People to Overcome Information Controls and Attacks

3D. FUNDING AGENCY OFFICIAL, IF ANY, TO BE NOTIFIED OF IRB APPROVAL

Last Name:	First Name:	Salutation:	
Agency:	Office Address:		Mail Code:
Street Address:	City:	State:	Zip Code:

[2] Clarify whether or not sponsor requires specific language in the contractual agreement that impacts human subjects research [2]
[3] Clarify whether or not the sponsor requires the protocol adhere to ICH GCP (E6) standards

Phone:	Fax:	E-mail:

4. FINANCIAL INTERESTS: Indicate below if any investigators or any members of their immediate families have any relationships, commitments, or activities with the sponsor of this research that might present or appear to present a conflict of interest with regard to the outcome of the research. (If a financial conflict of interest exists, please submit the University of Illinois approved conflict management plan. If you have questions about conflict of interest contact the Office of the Vice Chancellor for Research at 217-333-0034.)

☐ Ownership, equity or stock options
☐ Has been disclosed to the Illinois campus **OR** ☐ has not been disclosed to the Illinois campus

☐ Personal compensation such as royalties, consulting fees etc.
☐ Has been disclosed to the Illinois campus **OR** ☐ has not been disclosed to the Illinois campus

☐ Intellectual property such as patents, trademarks, copyright, licensing, etc.
☐ Has been disclosed to the Illinois campus **OR** ☐ has not been disclosed to the Illinois campus

☐ Other conflict of interest:
☐ Has been disclosed to the Illinois campus **OR** ☐ has not been disclosed to the Illinois campus

☒ No conflicts exist

5. SUMMARIZE THE RESEARCH. In **LAY LANGUAGE**, summarize the objectives and significance of the research.

Phishing is a social engineering technique used to gather sensitive information (passwords, credit card numbers, SSNs, etc.) by disguising as a legitimate entity in electronic communication, typically email. Phishing is a common and growing occurrence—an estimated three-quarters of all organizations [1] were targeted by phishing in 2016 alone, accounting for $9 billion in losses [2]—and institutions of higher education are no exception. Within the last year, employee paychecks at Illinois State University [3] and Kansas University [4] were stolen through phishing.

As researchers, we seek to examine user susceptibility to phishing attacks. In particular, we will study how the presence/absence of network security protocols (e.g. HTTPS and email over TLS) influence the effectiveness of phishing campaigns. Additionally, we seek to understand whether there is a misalignment between the security properties that HTTPS and email over TLS actually provide versus the protection that users think they provide. By measuring the likeliness of users to fall for phishing, we can measure how much they trust or distrust certain security protocols. Ultimately, understanding the causes of phishing vulnerability will inform the development of more effective anti-phishing tools and user education.

[1] https://info.wombatsecurity.com/state-of-the-phish
[2] https://www.rsa.com/en-us/blog/2016-12/2017-global-fraud-cybercrime-forecast
[3]http://www.pantagraph.com/news/local/data-breach-results-in-misdirected-payroll-at-isu/article_71bdd022-90dd-5a2b-bd84-11467982b13c.html
[4]http://www.kansas.com/news/local/crime/article88960532.html

6. PERFORMANCE SITES

Including Urbana-Champaign sites, describe ALL the research sites for this protocol. For each non-Urbana-Champaign site, describe: Whether the site has an IRB. Whether the site has granted permission for the research to be conducted. Contact information for the site. If the site has an IRB, whether the site's IRB has approved the research or planned to defer review to a University of Illinois IRB.		For non-Illinois sites, documentation of IRB approval is:
1.	UIUC	☐ Attached ☐ Will Follow ☒ N/A
2.	Internet (SurveyMonkey)	☐ Attached ☐ Will Follow ☒ N/A
3.		☐ Attached ☐ Will Follow ☐ N/A

List and describe any additional Performance Sites information on an attachment and check here: ☐

7. DESCRIBE THE HUMAN SUBJECTS

7A. SECONDARY DATA ONLY? If this research *only* involves the analysis of data that *has already been collected* from human subjects and *no new data collection will occur,* check here: ☐

7B. MATERIALS OF HUMAN ORIGIN? Will this research involve the collection, analysis, or banking of human biological materials (*e.g.,* cells, tissues, fluids, DNA)? ☐ **Yes** ☒ **No**

If yes attach **Appendix C**, the *Biological Materials Form*.

7C. ANTICIPATED NUMBERS How many subjects, including controls, will you study in order to get the data that you need?

If you plan to study disproportionate numbers of a given sex, race, or minority group, provide scientific rationale in Part 11.

Performance Site		**# Male**	**# Female**	**Total**
1.	Technology Services	Up to 270	Up to 270	Up to 270
2.				
3.				
TOTALS		Up to 270	Up to 270	Up to 270

List Anticipated Numbers for additional Performance Sites on an attachment and check here: ☐

7D. AGE RANGE Mark all that apply. Researchers planning to include children in research projects involving *more than minimal risk* must provide written documentation of the benefits that are likely to accrue to a child participating in the project. This should include information gathered on adults, if it exists, or an explanation about why it does not exist.

[ ] 0–7 years **[ ]** 8–17 years **[X]** 18–64 years **[X]** 65+ years

→ ☐ If applicable, written documentation of benefits for including children in ***more than minimal risk*** research is attached.

7E. SPECIAL OR VULNERABLE POPULATIONS Mark groups that will be targeted by design. Also indicate groups likely to be involved in the research even though they are not targeted by design.

☒ None of the following special populations will be targeted

☐ Children (age < 18)
☐ Neonates
☐ Fetuses *(in utero)*
☐ *in vitro* fertilization
☐ Pregnant or lactating
☐ Inpatients
☐ Outpatients
☐ Elderly (age > 65)
☐ Mentally disabled or cognitively impaired persons
☐ Adults with legal guardians
☐ Persons with limited civil freedom (*e.g.,* prisoners)
☐ Specific racial or ethnic group(s)—
☐ Low income or economically disadvantaged persons
☐ Illinois Students—name subject pool, if
☐ Other College Students—name subject

☐ Other (describe here):

7F. if you checked any of the groups in question 7E, describe additional safeguards included in the protocol to protect the rights and welfare of special or vulnerable populations.

8. RECRUITMENT

8A-1 RECRUITING PROCEDURES specifically describe the systematic procedures for finding and recruiting subjects or requesting pre-existing data or materials. 1) State whether any of the researchers are associated with the subjects (*e.g.,* subjects are students, employees, patients). 2) Name any specific agencies or institutions that will provide access to subjects or subject data. 3) Who will contact the prospective subjects? 4) Who gives approval if subjects are chosen from records? 5) Describe solicitation through the use of advertising (*e.g.,* posters, flyers, announcements, newspaper, radio, television, Internet), face-to-face interaction, direct mail or phone contact, classrooms, subject pools, health care registries, patient referrals, and institutional "gatekeepers," as applicable.

Technology Services at Illinois is responsible for supporting and improving the technological security of university members and assets. To accomplish these duties, they are authorized to perform routine security auditing, testing, and awareness campaigns for the members of the university. Our proposed study will develop a phishing drill that will be deployed and operated by Technology Services to understand the security posture of university members.

This study targets all Technology Services employees as part of employee phishing training. We are coordinating the study with the following Technology Services employees: Taylor Judd (Privacy and Information Security Specialist) and Eric Frahm (Lead Application Specialist). These subjects, along with the security team (Jeremy Watson, Robert Heren, Carl Stephens, Prabha Manda, Charles Geigner) will have prior knowledge of the research efforts and will be excluded from the results. Taylor Judd and Eric Frahm will henceforth be referred to as "Technology Services collaborators" and are not included as part of the research team. They will have exclusive control of the research apparatus and access to PII as entailed by their employment roles. The research team will not have access to the research apparatus and will only receive anonymized results – see section 18B "Data Collection" for details.

Taylor Judd will provide a list of subject names and email addresses; however, this data will NOT be made available to researchers. Technology Services collaborators will operate the research apparatus that contacts research subjects via a phishing email. After running the phishing exercise, only anonymized results will be exported to the researchers.

Approval to choose all Technology Services employees is given by Joseph Barnes, the Chief Privacy & Security Officer at UIUC. He has signed-off (see attached) on running this research experiment as part of employee security training. There is no solicitation or advertising, since participants are automatically selected for the study. We have also received approval from Elyne Cole, the Associate Provost for Human Resources at the University of Illinois at Urbana-Champaign (attached). Mark Henderson, the Chief Information Officer at the University of Illinois at Urbana-Champaign, has also been informed of the study (attached).

8 A-2 Attach final copies of recruiting materials including the final copy of printed advertisements and the final version of any audio/taped advertisements and check here:
Attached ☐ Will Follow ☐

8B. WITHHELD INFORMATION Do you propose to withhold information from subjects prior to or during their participation?
☒ Yes ☐ No

If yes, describe what will be withheld, justify the withholding (address risks, provide rationale), describe the debriefing plan, and attach a labeled copy of a written debriefing form, to be provided to subjects. ☒ Debriefing Attached ☐ Will Follow

Participants will be presented with a forged email from University of Illinois' Technology Services as well as a forged login page that will mimic a legitimate University of Illinois login page. Our research goal is to understand how participants respond to such emails and websites. Informing participants that the email and login pages are forgeries would bias their decision whether to trust the pages and would render the experiment useless.

By withholding information from participants, we do not incur any risk of PII / private data loss because we design the phishing tool to be completely anonymized to the researchers and prevent the phishing website from transmitting credential information over the network. Instead, the only information transmitted is whether the username and password fields contained "valid," "invalid," or "empty" values (according to university username/password restrictions) when the user tries to submit their credentials. The primary risk involved is that Technology Services will know which employees are susceptible to phishing, which may have a negative impact on a participant's reputation. To address this risk, we allow users who are successfully phished (i.e. those who submit their credentials) to immediately opt out of the study and have all identifying information removed.

We will debrief participants of the study in two ways, depending on the nature of their participation. For those that go through the entire phishing workflow from email, to website, to credential submission, we will immediately direct them to an informed consent page (attached) that provides debriefing information as well as an option to opt out of the study. To inform the other participants who do not fall for the full phishing drill, we will send an email to all Technology Services employees

within seven days of experiment deployment that includes a summary of the research as well as a link to a second webpage with debriefing information. This second debrief site (attached) differs from the first debrief site in two ways. First, the debrief site for participants who did not fall for the phishing experiment does not include survey information, since the survey is only meant for those who were successfully phished. Second, the site does not provide participants the option to opt out, since they did not demonstrate susceptibility and would not be subject to the same potential mental distress as a susceptible participant. The research summary text for the notification email is included below:

"The email titled 'Network Abuse Warning' that was sent to you on <DATE> from krandolph@illinois.edu was part of a phishing experiment conducted jointly by Technology Services and the Network Security Research Group (NSRG). The phishing test was conducted as part of an ongoing effort to assess employee security behavior and to improve employee security education. For more information on the research study and educational materials, please visit <DEBRIEF_SITE_2>."

8C. PROTECTED HEALTH INFORMATION (PHI) The IRB must address the privacy and use of health information that is created, received, or housed by health care providers, health plans, or health care clearinghouses and that identifies or could be used to identify an individual. During *either recruiting or data collection*, will you use or have access to such information that is related to the past, present or future health or conditions of a *living or deceased* individual, provision of health care to the individual, or the payment for the provision of health care to the individual? ☐ Yes ☒ No

8D. SCHOOL-BASED RESEARCH If subjects will be recruited from Illinois public or private elementary or secondary schools, additional deadlines and procedures apply. Criminal background clearances might be required. Special consideration must be given to the exclusion of protected populations. Please contact the Office of School–University Research Relations (OSURR) (217.244.0515 or http://www.ed.uiuc.edu/BER/OSURR.html) for more information. Mark one:

☐ Illinois schools **will** be used ☒ Illinois schools **will not** be used

9. INCLUSION AND EXCLUSION CRITERIA Address all four of the following items in explaining who will and will not qualify for participation and how that determination will be made: (1) Describe procedures to assure equitable selection of subjects. Justify the use of any special or vulnerable groups marked in Part 7E. Selection criteria that target one sex, race, or ethnic group require a clear scientific rationale. (2) List specific criteria for inclusion and exclusion of subjects in the study, including treatment groups and controls. (3) Name and attach copies of measures and protocols that will be used to screen applicants. (4) Explain how the inclusion/exclusion criteria will be assessed and

by whom. If special expertise is required to evaluate screening responses or data, tell who will make this evaluation and describe their training and experience.

We will involve all employees of the Technology Services office at UIUC, excluding those already informed (listed in Section 8A-1). There is no screening involved. Our treatment groups and controls will be randomly selected.

10. RESEARCH PROCEDURES: Using LAYMAN'S LANGUAGE, specifically describe what the participants (treatment groups and controls) will do and where the research activities will take place. Give approximate dates and durations for specific activities, including the total number of treatments, visits, or meetings required and the total time commitment.
(For schools-based research where class time is used, describe in detail the activities planned for nonparticipants and explain where (*e.g.,* in a classroom, in a private area) both participants and nonparticipants will be located during the research activities. Include a concise description of procedures, locations, time commitments, and alternate activities on the relevant consent and assent forms.)

The study involves investigating the effect of two binary features: sending a phishing email over an encrypted/unencrypted channel and including an HTTP/HTTPS link in the phishing email. As such, we employ 4 distinct test groups: 1) one that receives a phishing email with HTTP link over an unencrypted channel (i.e. the control group), 2) one that receives a phishing email with HTTP link over an encrypted channel, 3) one that receives a phishing email with HTTPS link over an unencrypted channel, and 4) one that receives a phishing email with HTTPS link over an encrypted channel. The experimental activities for each group are identical.

We have built a research apparatus server for sending phishing emails and tracking phishing results. We will provide this apparatus to our Technology Services collaborators, and it will be configured so that none of the researchers have login access to the tool or access to the servers that it is running on. The Technology Services collaborators will operate the experiment once we have received IRB approval (tentatively early March). The first step is to send a phishing email (attached) to all Technology Services employees that warns recipients that their device has been potentially compromised. The email originates from the address krandolph@illinois.edu and purports to be sent from Kevin Randolph, a fictitious Legal Compliance Officer employed by Technology Services. In order to prevent their device from being banned from the campus network, the email instructs recipients to click or copy/paste a link to log in and verify device ownership. The phishing email only takes about 1 minute to read, if the participant decides to open it at all.

The login link leads to the phishing website (attached), which is hosted at illinois-abuse.net, and presents a visual clone of Shibboleth, the familiar single sign-on service used by several university

web services. If a user attempts to login with a username and password, these sensitive credentials are redacted in the browser and replaced with one of three values, based on the length of the username and password: “valid” according to university restrictions on username and password lengths, “invalid”, and “empty.” Only these non-identifying, non-sensitive values are transmitted to the research server, and upon receipt, the phishing website immediately redirects the participant to the debriefing page.

The debriefing page (attached) provides an informed consent section that allows users to opt out of the research study and have their results obscured from Technology Services (all results given to the research team are by default anonymized). A link to educational material from Technology Services is provided to help participants decrease their future phishing susceptibility.

The debrief page also contains a link to an optional follow-up survey hosted on SurveyMonkey that awards users $10 for successful completion of the survey. Only those who fall for the phishing scam are eligible to take the survey. The survey (attached) consists of general demographic questions, questions to understand why participants were vulnerable to phishing, and several standardized questions for quantifying computer security expertise, internet usage, and overall risk behavior. Based on the general consensus [5][6][7][8] that respondents can answer 2-4 questions a minute, and a survey dry run performed by the researchers, we expect the survey to take approximately 20-25 minutes to complete.

[5] http://question-science.blogspot.com/2012/07/how-to-calculate-length-of-survey.html
[6] http://www.amplituderesearch.com/online-market-research-article.shtml
[7] https://fluidsurveys.com/university/finding-the-correct-survey-length/
[8] https://www.surveymonkey.com/blog/en/blog/2011/02/14/survey_completion_times/

11. EQUIPMENT Will any physical stimulation or physiological data acquisition equipment be used with the subjects?

☐ Yes ☒ No If yes, attach **Appendix A**, the *Research Equipment Form.*

12. DEVICES Will any devices be used with the subjects?

☐ Yes ☒ No If yes, attach **Appendix B-1,** the *Device Form*.

13. DRUGS AND BIOLOGICS Will any drugs or chemical or biological agents be used with the subjects?

☐ Yes ☒ No If yes, attach **Appendix B-2**, the *Drug and Chemical Usage Form*.

14. MRI AT BIC To use the Beckman Institute Biomedical Imaging Center (BIC) in human subject's research, you must obtain *prior approval* from the BIC (217.244.0600; bmrf@bmrl.bmrf.uiuc.edu) and use BIC-approved screening and consent forms. Attach:

BIC approval ☐ Attached
BIC screening form ☐ Attached
BIC consent form ☐ Attached

15. MEASURES If subjects will complete questionnaires, surveys, interviews, psychological measures, or other measures, however administered, the IRB must review and approve the measures. List all such measures here and attach complete, labeled copies (including translations, if applicable) to this application:

Measure 1:	Phishing Email	☒ Attached ☐ Will Follow
Measure 2:	Debriefing Page	☒ Attached ☐ Will Follow
Measure 3:	Survey	☒ Attached ☐ Will Follow
Measure 4:		☐ Attached ☐ Will Follow

List additional Measures on an attachment and check here: ☐

16. SUBJECT REMUNERATION

Will subjects receive inducements or rewards before, during, or after participation?
☒ Yes ☐ No

If yes, will payment be prorated for partial participation?
☐ Yes ☒ No

If remuneration will be given, for each subject group:

(1) Specify the form of remuneration, including $, course credit, lottery, gift certificate, or other;
(2) State the $ amount or the approximate $US value, or the course credit and its percentage of the final grade;
(3) Explain the remuneration plan, including whether and how prorating will be made for partial participation;
(4) For lotteries, include (a) the number of prizes, (b) the nature and value of each prize, (c) the approximate odds of winning, (d) the date(s) of the drawing(s), and (e) how winners will be notified, by whom, and by when; and
(5) Include all this information on the relevant consent forms.

Participants who are successfully phished will be offered a $10 Amazon gift card for successfully completing the follow-up survey. Partial survey participation will not be prorated. Users who opt out of the study will not be provided any remuneration. The information above will be provided on the debriefing page alongside a link to the actual survey.

17. SUBJECT OUTLAY Will subjects incur costs for research-related procedures (*e.g.*, longer hospitalization, extra tests), use of equipment, lost compensation, or transportation (over 50 miles)?
☐ Yes ☒ No If yes, describe here:

N/A

18. CONFIDENTIALITY OF DATA Answer each of the following to describe methods that will ensure the confidentiality of individually identifiable data. Confidentiality is required unless subjects give express, written permission to have their identifiable information published, presented, or shared.

18A. CHECK IF USED IN DATA COLLECTION: ☐ Audio tapes/digital voice ☐ Video tapes

☐ Still photos ☐ Other imaging

18B. DATA COLLECTION Explain how the data will be collected. If anonymous data collection is proposed, provide details of how investigators *will not have the ability to trace responses to subject identities.* For multiphase data collection or if multiple contacts will be made with subjects, specifically explain the subject tracking and coding systems.

Address the confidentiality of data collected via e-mail, databases, Web interfaces, computer servers, and other networked information, as applicable.

Technology Services collaborators will collect data through webserver access logs to track when participants open phishing emails, access the phishing website, and submit participant credentials. Prior to the deployment of the experiment, each participant is assigned a random pseudonymous identifier that will be attached to each web request for the purposes of tracking individual participants. No personally identifiable information is ever transmitted to the research apparatus webserver, so an outsider observing traffic on the network will not be able to link the anonymous identifier to a participant. Only a registered operator (i.e. Technology Services collaborators) with

access to the secure webserver (see Section 18C) will be able to de-anonymize participants. Researchers will NOT have access to the secure research apparatus and will only receive anonymized results, with email address, names, and IP addresses removed.

We will be using SurveyMonkey, a survey platform, to administer all surveys directly. SurveyMonkey supports sending data over an encrypted HTTPS connection (using TLS) and will be configured so that we do not trace any respondent IP addresses. The survey questions do not ask for any personally identifying information.

18C. DATA SECURITY Describe how and where the data be kept so that the data remain confidential.

Technology Services will use Amazon EC2 for operating the research apparatus and storing raw data. They will export anonymized data to NSRG servers for research analysis. For both collection locations, risks will be severely curtailed through the use of best practices in securing the collection infrastructure and processing machines. These include, but are not limited to Locked data center, Restricted access, Restrictions on copying study-related materials, Audit logs for accessing study-related data, Access rights terminated when authorized users leave the project or unit, Individual ID plus cryptographic key protection, Encryption of digital data, Network restrictions, No non-UI devices are used to access project data, Security software (like a firewall) is installed and regularly updated on all servers, workstations, laptops, and other devices used in the project.

18D. STAFF TRAINING Describe the training and experience of all persons who will collect or have access to the data.

All persons who will collect or have access to this data have experience performing academic research or are working for experienced researchers. The responsible primary investigator (Michael Bailey) has published over 60 academic papers, many of which involve human subjects and thus IRB approval. The secondary investigator (Zane Ma) is a third-year graduate student who has spent three years performing academic research under faculty at the University of Illinois. Other investigators are research scientists, graduate, and undergraduate students at the University of Illinois who are working with Michael Bailey and Zane Ma. All investigators have completed the IRB Required Social Behavioral Core CITI training modules.

18E. DATA RETENTION How long will the data be kept?

Data will be kept in accordance with the data retention policy of the NSRG which states that all data will be deleted after 3 years.

18F. DISSEMINATION OF RESULTS what is (are) the proposed form(s) of dissemination (*e.g.,* journal article, thesis or academic paper, conference presentation, sharing within industry or profession)?

The results of this experiment will be disseminated in paper submission(s) to a computer security research conference. The results will also be disseminated internally to the University of Illinois' Technology Services department to improve phishing resilience.

18G. PRIVACY Describe provisions to protect the privacy interests of subjects.

All questions in our surveys contain an option titled "Prefer not to answer." Subjects may choose this option if they do not wish to share information about the question. None of the survey questions contain personally identifying information — the demographic questions asked are very general.

Data will be anonymized by removing emails and names before analysis or sharing to protect the interests of Technology Services employees who are subject to the phishing experiments. Only a random pseudonymous identifier will be used for each subject to link phishing vulnerability and survey results.

18H. INDIVIDUALLY IDENTIFIABLE INFORMATION Will any individually identifiable information, including images of subjects, be published, shared, or otherwise disseminated? ☐ Yes ☒ No

If yes, subjects must provide explicit consent or assent for such dissemination. Provide appropriate options on the relevant consent documents.

19. INFORMED CONSENT: University policy requires the execution of a comprehensive, written document that is signed by the subject (or the subject's authorized representative) as the principal method for obtaining consent from subjects. The language in the document must be understandable to the subject or the subject's legally authorized representative.

An investigator may request a Waiver or Alteration of Informed Consent or a Waiver of Documentation of Informed Consent (e.g., online consent, oral consent). If requesting a waiver please complete the appropriate waiver form at: www.irb.illinois.edu and submit it with the New Protocol Application form for review.

Children must *assent* (or, voluntarily agree) to participation and a parent must separately consent on behalf of their child (*i.e.,* two different forms are generally required). Children under age 8 may assent either orally or passively, depending on their level of maturity. Children 8–17 years old should sign a written form unless the University of Illinois at Urbana-Champaign IRB approves a different process.

19A. TYPE OF CONSENT Check all that apply and attach one copy of each relevant form, letter, or script on university letterhead. Include translations, if consent will be obtained in a foreign language. Use headings, headers, or footers to uniquely identify each document and associate it with the subject group for which it will be used.

☐ **Written informed consent (assent) with a document <u>signed by</u>**
☐ adult subjects ☐ parent(s) or guardian(s) ☐ adolescents aged 8–17 years

☒ **Waiver or Alteration of Informed Consent (Attach waiver form.)**
☒ adult subjects ☐ parent(s) or guardian(s) ☐ adolescents aged 8–17 years

☐ **Waiver of Documentation (signature) of Informed Consent (Attach waiver form.)**
☐ adult subjects ☐ parent(s) or guardian(s) ☐ adolescents aged 8–17 years

19B. USE OF PROXY Will others (*e.g.,* next of kin, legal guardians, powers of attorney) act on behalf of adult subjects in giving consent to participate in this research? ☐ Yes ☒ No (if yes, describe in Section 20D.)

19C. USE OF PROXY OUTSIDE THE UNITED STATES If a proxy is used in research conducted outside Illinois, provide justification (e.g., statement of an attorney or copy of applicable law) that the proxy is authorized under the laws of the jurisdiction in which the research will be conducted to consent to the procedures involved in this protocol.

N/A

19D. CONSENT PROCESS Describe when and where voluntary consent will be obtained, how often, by whom, and from whom. If cognitively impaired subjects (including children under age 8) will be involved, explain how the subject's understanding will be assessed and how often; include the questions that will be asked or actions that will be taken to assess understanding.

Describe any waiting period between informing the prospective subject and obtaining the consent. Describe steps taken to minimize the possibility of coercion or undue influence. Indicate the language used by those obtaining consent.
Indicate the language understood by the prospective subject or the legally authorized representative.

If the research involves pregnant women, fetuses, or neonates, indicate whether consent will be obtained from the mother, father, or both. If the research involves children, indicate whether consent will be obtained from: Both parents unless one parent is deceased, unknown, incompetent, or not reasonably available, or when only one parent has legal responsibility for the care and custody of the child; or from one parent regardless of the status of the other parent.

Please see the attached petition for a waiver of informed consent. In summary:

This research involves no more than minimal risk. All subjects will be debriefed, with two separate debriefing mechanisms. Subjects who fall for the phishing drill will receive immediate debriefing via a debriefing webpage that provides the ability to opt out of the study. Subjects who do not fall for phishing will be debriefed within a week, at latest, of phishing deployment via an email that summarizes the research and provides a link to a more detailed debriefing webpage.

All subjects have already consented to the UIUC Acceptable Use Policy and their employment contracts. Technology Services employees, i.e. the study subjects, are responsible for protecting information: our research involves an employer auditing its defensive preparedness. Informed consent before participating in the phishing study would severely bias results.

20. RISKS

20A. DESCRIPTION specifically describe all known risks to the subjects for the activities proposed and describe the steps that will be taken to minimize the risks. Include any risks to the subject's physical well-being, privacy, dignity, self-respect, psyche, emotions, reputation, employability, and criminal and legal status. Risks must be described on consent forms.

To provide a comprehensive view of the risks of our proposed research, we break down the risks for each entity involved in the research process.

<u>Study Participants (Technology Services Employees):</u>
Demonstrated susceptibility to the phishing experiment may influence the reputation of a participant, which may affect their professional or academic standing with the university. We plan to mitigate this concern by allowing participants to opt out of the study and have their results obscured from Technology Services collaborators by removing all PII. We also note that the study is part of routine technology security training for all Technology Services employees, and the Technology Services collaborators who are operating the research apparatus are the only individuals with access to this information and perform similar training / testing as part of their normal employment. As discussed in Section 18C, data security follows best practices and reduces the risk of attacker infiltration to no more than minimal.

Individual participants in the study are also asked to take an optional follow-up survey. Some of the questions inquire about participant security behavior. If the data in this study were to be compromised, then a digital attacker could capitalize on this knowledge and understand the most effective ways to compromise respondents, which could cause financial loss and distress. Some of the questions also ask the respondent about the likelihood or frequency of hypothetically engaging in activities that are considered morally objectionable or illegal (e.g. viewing adult content or purchasing controlled substances online). These questions could themselves cause distress, or knowledge of the responses could jeopardize the respondent's reputation/employability/legal standing. We mitigate these risks by allowing participants to select "Prefer not to respond" for any and all questions, and also allow them to quit the survey at any time. Furthermore, we believe the risk of survey data compromise is minimal because 1) the survey is conducted on SurveyMonkey, a trusted platform with strong security policies, 2) we collect as little identifying data as possible, and 3) we do not attempt to de-anonymize the data.

Participants who fall for the phishing experiment may experience distress and spend additional time and attention when handling future emails. We argue that this is a benefit of the phishing drill from the perspective of Technology Services, which seeks to improve operational security. However, to best translate this distress into productive caution, we provide participants with educational materials on the debriefing page that instruct them on how to effectively and efficiently analyze such emails and websites in the future.

Help Desk / IT Support Team

The tech support team may be overwhelmed with support requests asking about the phishing email or phishing website. However, we expect no more than minimal disturbance, since we are only sending out emails to at most 270 individuals.

University Digital Infrastructure

Sending phishing emails from a university email address could cause third party software (e.g. anti-virus, email clients, web browsers) to blacklist the email address, either through automatic detection or manual reporting by users. Using a real user's email address to send out email would cause potential distress, limit a user's legitimate email communications, and potentially harm the sender's reputation, both personal and digital. Instead we create an email address krandolph@illinois.edu for a fictitious user, Kevin Randolph, for the sole purpose of the research experiment. We intentionally choose an email address that is one character longer than permitted email addresses so that future users of the email system cannot inherit the email address and the negative reputation that may come with it.

A phishing website is subject to similar risks – it can be added to blacklists by third party software, rendering the website domains and related subdomains useless. To avoid this risk, we purchased a separate domain for hosting the phishing website: illinois-abuse.net. Even if this domain is blacklisted, there should be no negative effects on any legitimate Illinois web domains.

20B. RISK LEVEL: ☒ **No more than minimal risk**
(The probability and magnitude of harm or discomfort anticipated for participation in the proposed research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests).

☐ **More than minimal risk**

20C. Data Monitoring Plan: If you checked that the research is more than minimal risk, describe the provisions for monitoring the data to ensure the safety of subjects (Who will periodically monitor harms and benefits experienced by subjects to ensure that the relationship of risks to potential benefits remains unchanged? How often will monitoring occur? What analyses will be performed? If appropriate, what criteria will be used to stop the research based on monitoring of the results?)

N/A

21. BENEFITS Describe the expected benefits of the research to the subjects and/or to society.

The University of Illinois email system and all large email systems are regularly targeted by phishing campaigns. Automated tools can block many of the attacks, but none are completely foolproof. This phishing experiment will provide the immediate short-term benefit of helping the University better understand its susceptibility to phishing, and it will educate Technology Services employees on how to avoid future malicious phishing attacks, keeping University systems and secrets secure. More broadly, our research will help to understand the trust models behind users' evaluation of whether an email is safe to interact with. This will allow Technology Services to provide better warnings, indicators, and training. Our results will also inform improved anti-phishing measures for other organizations as well.

In the long-term, we hope to examine whether users place undue trust in security protocols that do not actually provide any notion of trust – they only provide confidentiality, integrity, and name-based authentication. If so, we can begin to make the case for re-aligning users' assumptions of security and the properties actually afforded by security protocols. Ultimately, we wish to build

systems that treat trustworthiness as a first-class security property that will help combat a broad range of digital attacks.

22. RISK/BENEFIT ASSESSMENT Weigh the risks with regard to the benefits. Provide evidence that benefits outweigh risks.

To summarize, the primary risks of the study are the harms caused by loss or de-anonymization of sensitive data and the psychological distress associated to falling for phishing. We believe that the best-practice security procedures we put in place (e.g. physical/digital access control, encryption, auditing) minimize the risk of data loss. Furthermore, by preventing researchers from accessing any de-anonymized data and isolating sensitive data to only Technology Services collaborators, we minimize the risk of participant privacy violations. The remaining risk of psychological distress is hard to predict, but we curtail it by allowing participants to opt out of the study and translating the distress into improved phishing education.

The primary benefits of the study are for Technology Services to learn the current susceptibility of its employees to phishing, provide phishing education for those employees, and to better model users' decision making around potential phishing situations, specifically in the context of user assumptions of the guarantees provided by security protocols. The broader benefit of this research would make the case for building trustworthiness as a first-class security property. Trustworthiness, in turn, would allow for automated, delegated security decision making that would help mitigate attack scenarios enabled by poor manual decision making. If trustworthiness makes even a dent in the projected $2 trillion of losses in cybercrime by 2019 [9], then the benefits far exceed the risks.

[9] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

If additional Risk/Benefit information is attached, check here: ☐

23. Is this a multi-center study in which the Illinois investigator is the lead investigator of a multicenter study, or the University of Illinois at Urbana-Champaign is the lead site in a multi-center study.

Yes ☐ **No** ☒

If yes, describe the management and communication of information obtained that might be relevant to the protection of subjects, such as: unanticipated problems involving risks to subjects or others, interim results and protocol modifications.

N/A

24. INVESTIGATOR ASSURANCES: The signature of the Responsible Project Investigator is required (scanned or faxed signatures are acceptable). Other investigators are also responsible for these assurances and are encouraged to sign.

I certify that the information provided in this application, and in all attachments, is complete and correct.

I understand that I have ultimate responsibility for the protection of the rights and welfare of human subjects, the conduct of this study, and the ethical performance of this project.

I agree to comply with all Illinois policies and procedures, the terms of its Federal Wide Assurance, and all applicable federal, state, and local laws regarding the protection of human subjects in research.

I certify that

- The project will be performed by qualified personnel according to the University of Illinois at Urbana-Champaign IRB-approved protocol.
- The equipment, facilities, and procedures to be used in this research meet recognized standards for safety.
- No change will be made to the human subjects protocol or consent form(s) until approved by the University of Illinois at Urbana-Champaign IRB.
- Legally effective informed consent or assent will be obtained from human subjects as required.
- Unanticipated problems, adverse events, and new information that may affect the risk–benefit assessment for this research will be reported to the University of Illinois at Urbana-Champaign IRB Office (217.333.2670; irb@illinois.edu) and to my Departmental Executive Officer.

- I am familiar with the latest information concerning IRB regulations and policies available at www.irb.illinois.edu, and I will adhere to the policies and procedures explained therein.

- Student and guest investigators on this project are knowledgeable about the regulations and policies governing this research.

- I agree to meet with the investigator(s), if different from myself, on a regular basis to monitor study progress.

- If I will be unavailable, as when on sabbatical or other leave, including vacation, I will arrange for an alternate faculty sponsor to assume responsibility during my absence. I will advise the Illinois IRB by letter of such arrangements.

I further certify that the proposed research has not yet been done, is not currently underway, and will not begin until IRB approval has been obtained.

Responsible Principal Investigator	3/15/18 Date	Investigator	03/15/2018 Date
Investigator	3/15/18 Date	Investigator	03/15/2018 Date
Investigator	03/15/2018 Date	Investigator	Date

25. (OPTIONAL) DEPARTMENTAL ASSURANCE To be completed by the RPI's Departmental Executive Officer or their designee.

The activity described herein is in conformity with the standards set by our department and I assure that the principal investigator has met all departmental requirements for review and approval of this research.

Departmental Executive Officer (or designee) Date

* For units that conduct **scientific merit review,** the signature above documents the following:

☐ 1. The research uses procedures consistent with sound research design.
☐ 2. The research design is sound enough to yield the expected knowledge.

RESEARCH TEAM APPLICATION

Form to Report All Investigators That Will Participate in Any Way on The Research

IRB Number: 18554
Responsible Project Investigator: Michael Bailey

Project Title:

The Impact of Security Protocols on Phishing Efficacy

☐ Submitting with Initial New Protocol Application
☒ Changing research team, date of submission 03/15/2018

List all investigators engaged in the research study, including those from other institutions. Include all persons who will be 1) directly responsible for the project's design or implementation, 2) recruitment, 3) obtain informed consent, 4) involved in data collection, data analysis, or follow-up.

Collaborators, outside consultants, and all graduate and undergraduate students should be listed if they will be responsible for these activities. Include all investigators named on grant proposals who will be engaged in human subjects' research.

Note: Changes made to the Responsible Project Investigator require a revised New Protocol application and amendment form.

Please copy and paste text fields to add additional researcher team members.

Last Name: Ma	First Name: Zane	Academic Degree(s):		
Dept. or Unit: CS	Office Address: Office 445		Mail Code:	
Street Address: 1308 W Main St	City: Urbana	State: IL	Zip Code: 61801	
Phone: 408-940-5670	Net ID: zanema2	E-mail: zanema2@illinois.edu		
Affiliation:	☐ Faculty ☐ Academic Professional/Staff ☒ Grad Student ☐ Undergrad Student ☐ Visiting Scholar, or ☐ Non-Illinois Affiliate of (Institution):			
Training	☒ CITI Training, Date of Completion, 09/18/2017 ☐ Additional training, Date of Completion,			
☒	Please check box if this individual should be copied on IRB correspondence			

Last Name: Reynolds	First Name: Joshua	Academic Degree(s): BS	
Dept. or Unit: Computer Science	Office Address: 445 CSL		Mail Code:

Street Address: 2107 Hazelwood Dr. Apt 102	City: Urbana	State: IL	Zip Code: 61801
Phone: 916-676-6076	Net ID: joshuar3	E-mail: joshuar3@illinois.edu	
Affiliation:	☐ University of Illinois Faculty ☐ Academic Professional/Staff ☒ Grad Student ☐ Undergrad Student ☐ Visiting Scholar, or ☐ Non-Urbana-Champaign campus Affiliate of (Institution):		
Training	☒ CITI Training, Date of Completion, 9/14/17 ☒ Additional training, Date of Completion[1], 4/13/17		
☒	Please check box if this individual should be copied on IRB correspondence		

Last Name: Dickinson	First Name: Joseph	Academic Degree(s):	
Dept. or Unit: ECE	Office Address: Office 445	Mail Code:	
Street Address: 1308 W Main St	City: Urbana	State: IL	Zip Code: 61801
Phone:	Net ID: jddicki2	E-mail: jddicki2@illinois.edu	
Affiliation:	☐ Faculty ☐ Academic Professional/Staff ☐ Grad Student ☒ Undergrad Student ☐ Visiting Scholar, or ☐ Non-Illinois Affiliate of (Institution):		
Training	☒ CITI Training, Date of Completion, 10/17/2017 ☐ Additional training, Date of Completion,		
☒	Please check box if this individual should be copied on IRB correspondence		

Last Name: Mason	First Name: Joshua	Academic Degree(s):	
Dept. or Unit: ITI	Office Address: Office 446	Mail Code:	
Street Address: 1308 W Main St	City: Urbana	State: IL	Zip Code: 61801
Phone:	Net ID: joshm	E-mail: joshm@illinois.edu	
Affiliation:	☐ Faculty ☒ Academic Professional/Staff ☐ Grad Student ☐ Undergrad Student ☐ Visiting Scholar, or ☐ Non-Illinois Affiliate of (Institution):		
Training	☒ CITI Training, Date of Completion, 03/05/2018 ☐ Additional training, Date of Completion,		
☒	Please check box if this individual should be copied on IRB correspondence		

INVESTIGATOR ASSURANCES

I certify that the information supplied on this form is complete and correct and that new members of the research team will not engage in research until IRB approval has been obtained.

Responsible Project Investigator _____ Date 3/15/18

For Office Use Only

[1] [1] Additional CITI modules may be required depending on subject populations or types of research. These include: (i) research enrolling children; (ii) research enrolling prisoners; (iii) FDA regulated research; (iv) data collected via the internet; (v) research conducted in public elementary/secondary schools; and, (vi) researchers conducted in international sites

Email Approval from Joe Barnes

From: Barnes, Joe
Sent: Tuesday, February 6, 2018 3:51 PM
To: Judd, Taylor Allen <tjudd@illinois.edu>
Subject: RE: Email Authorization for NSRG

To whom it may concern.

On behalf of the Office of the CIO, I am granting permission to NSRG to conduct phishing activities, as described in the IRB proposal, on Technology Services employees.

If there are any questions or concerns please don't hesitate to contact me directly.

Thanks
Joe

****
Joe Barnes, CISSP
Chief Privacy & Security Officer
Technology Services at Illinois
University of Illinois at Urbana-Champaign
jdbarns1@illinois.edu
(217) 265-6447

Email Approval from Elyne Cole / Mark Henderson

From: "Cole, Elyne G" <e-cole1@illinois.edu>
Subject: RE: Authorization of Study to be Conducted on Staff Members
Date: March 14, 2018 at 3:52:47 PM CDT
To: "Bailey, Michael Donald" <mdbailey@illinois.edu>, "Henderson, Mark" <mhenders@illinois.edu>
Cc: "Barnes, Joe" <jdbarns1@illinois.edu>, "Ma, Zane Zheng" <zanema2@illinois.edu>, "Reynolds, Joshua Tyler" <joshuar3@illinois.edu>, "Judd, Taylor Allen" <tjudd@illinois.edu>, "Dickinson, Joseph Dale" <jddicki2@illinois.edu>, "Lore, Michelle H" <lore@illinois.edu>, "Harvey, Teresa" <tharvey@illinois.edu>

Dear Mr. Bailey,

I am writing in response to your request for approval for an awareness study to determine the susceptibility of university users to phishing attacks. Thank you for providing us with the requested information. Your request can now be approved.

By way of this email, I am copying Mark Henderson, Chief Information Officer, and administrator for Technology Services, for acknowledgement of his awareness of this research within his unit.

Sincerely,

Elyne Cole
Associate Provost for
Human Resources

From: "Henderson, Mark" <mhenders@illinois.edu>
Subject: Re: Authorization of Study to be Conducted on Staff Members
Date: March 14, 2018 at 4:31:11 PM CDT
To: "Cole, Elyne G" <e-cole1@illinois.edu>, "Bailey, Michael Donald" <mdbailey@illinois.edu>
Cc: "Barnes, Joe" <jdbarns1@illinois.edu>, "Ma, Zane Zheng" <zanema2@illinois.edu>, "Reynolds, Joshua Tyler" <joshuar3@illinois.edu>, "Judd, Taylor Allen" <tjudd@illinois.edu>, "Dickinson, Joseph Dale" <jddicki2@illinois.edu>, "Lore, Michelle H" <lore@illinois.edu>, "Harvey, Teresa" <tharvey@illinois.edu>

I acknowledge my awareness of this initiative.

Mark

Mark D. Henderson
Chief Information Officer
University of Illinois, Urbana-Champaign

From: "Cole, Elyne G" <e-cole1@illinois.edu>
Subject: Re: Authorization of Study to be Conducted on Staff Members
Date: March 15, 2018 at 7:25:26 AM CDT
To: "Bailey, Michael Donald" <mdbailey@illinois.edu>
Cc: "Henderson, Mark" <mhenders@illinois.edu>, "Barnes, Joe" <jdbarns1@illinois.edu>, "Ma, Zane Zheng" <zanema2@illinois.edu>, "Reynolds, Joshua Tyler" <joshuar3@illinois.edu>, "Judd, Taylor Allen" <tjudd@illinois.edu>, "Dickinson, Joseph Dale" <jddicki2@illinois.edu>, "Lore, Michelle H" <lore@illinois.edu>, "Harvey, Teresa" <tharvey@illinois.edu>

Dear Michael,

My apologies for the confusion. It was my intent to provide approval and ask Mark for acknowledgment at the same time. We have Mark's approval and we support your moving forward.

Please let me know if you have any further questions.

Elyne Cole

Sent from my iPhone

> On Mar 14, 2018, at 8:13 PM, Bailey, Michael Donald <mdbailey@illinois.edu> wrote:
>
> Ms. Cole,
>
> It wasn't clear from your email whether you approved the study and were simply notifying Mr. Henderson or whether you were waiting to approve the study contingent on acknowledgement by Mr. Henderson (which we all just received). If you would kindly clarify, I can package your response to the IRB.
>
> Thank you,
>
> -* Michael

Sample Phishing Email

krandolph@illinois.edu Today at 2:02 PM

To: John Doe

Network Abuse Warning

K

Dear John,

This notice is being served as a warning that the computer registered to you (johndoe@university.edu) has been discovered attempting to make repeated connections to prohibited/illegal sites. Technology Services takes the misuse of the UNIVERSITY campus network seriously and will blacklist and report this device according to the terms of the Policy on Appropriate Use of Computers and Network Systems at the University. For more information or if you believe you have received this notification in error, please follow the link below.

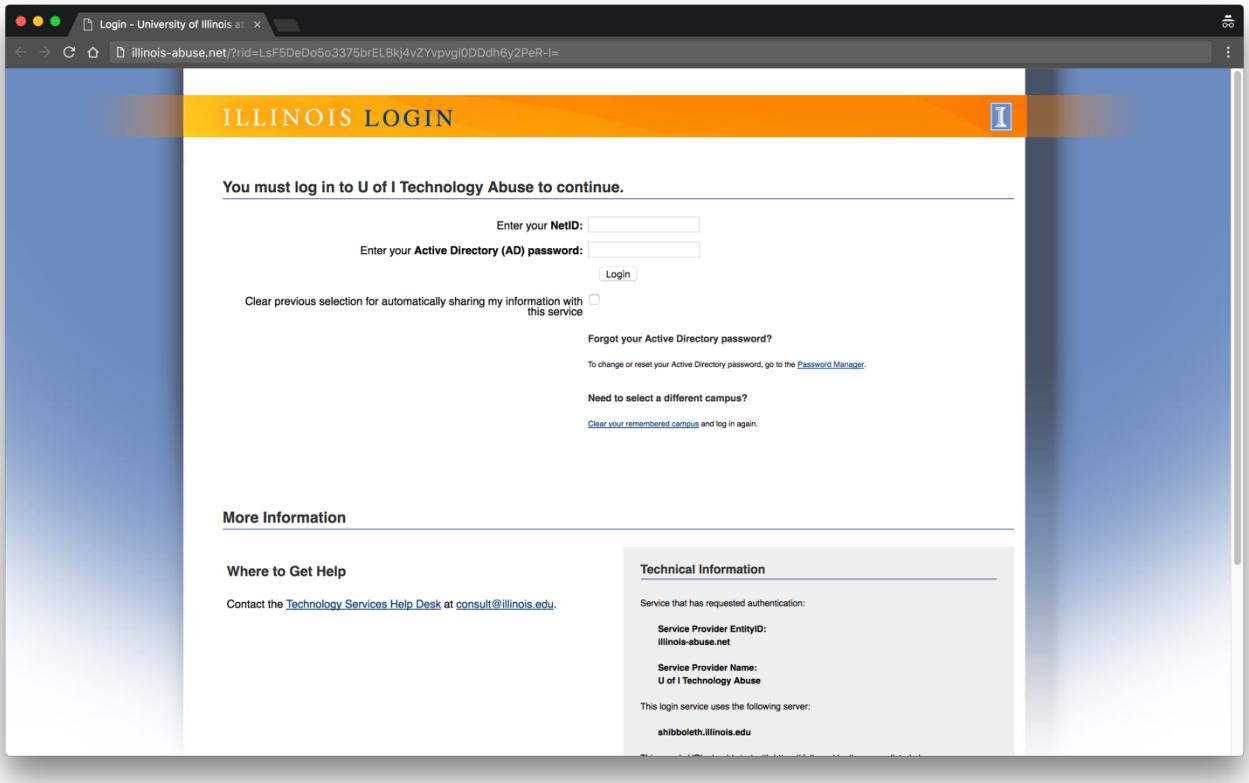
Follow this link or paste the following into your browser:
http://university-abuse.net/abuse-warning?rid=OfhqhSq4BpwCGpNOZYhgD6MEStOwgS-eqzEZUpTFvl4

-Kevin Randolph
Office of Technology Services
Legal Compliance Officer
krandolph@university.edu
(217)-555-1248

"You are never as important as when you are doing your job well"

TECHNOLOGY SERVICES

Sample Phishing Website



Follow-up Survey

Question or Question Category	Answer Options
Demographic	
Are you male or female?	Female, Male, Other, Prefer not to answer
What is your age?	17 or younger, 18-20, 21-29, 30-39, 40-49, 50-59, 60 or older, Prefer not to answer
What is the highest level of school you have completed or the highest degree you have received?	Less than high school degree, High school degree or equivalent (e.g., GED), Some college but no degree, Associate degree, Bachelor degree, Graduate degree, Prefer not to answer
Which of the following categories best describes your employment status?	Employed, working full-time; Employed, working part-time; Not employed, looking for work; Not employed, NOT looking for work; Retired; Disabled, not able to work; Prefer not to answer
Please select your affiliation with the University of Illinois, if any.	Faculty, Staff, Graduate Student, Undergraduate Student, No affiliation, Prefer not to answer
Prior Knowledge	
Had you heard any information about this specific research study in the past?	Yes, No, Prefer not to answer
Motivation	
Why did you open the phishing email?	*Open-ended*
Why did you click on the link in the phishing email?	*Open-ended*
Why did you enter your credentials on the phishing website?	*Open-ended*
What security indicators did you notice in the phishing email?	HTTP/HTTPS URL, URL bar lock icon, Other (please specify), None, Prefer not to answer
What security indicators did you notice on the phishing website?	HTTP/HTTPS URL, URL bar lock icon, Other (please specify), None, Prefer not to answer
{If indicator specified} What does the {security indicator} you noticed in the phishing email mean to you?	*Open-ended*
{If indicator specified} What does the {security indicator} you noticed on the phishing website mean to you?	*Open-ended*
Computer Expertise/Usage	
On average, how much time do you spend on the Internet per week (e.g., searching for information, checking email, streaming videos)?	Less than 10 hours, More than 10 but less than 30 hours, More than 30 but less than 50 hours, More than 50 but less than 80 hours, More than 80 hours, Prefer not to answer
Select the task(s) that you have previously accomplished; if none of these tasks applies to your situation, then please select “None of the above”	I have installed or re-installed an operating system on a computer, I have configured a home network, I have created a web page, None of the above, Prefer not to answer

For each of the following statements, please indicate how frequently you engage in the behavior described	
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	Never (1), Rarely (2), Sometimes (3), Often (4), Always (5), Prefer not to answer
I use a password/passcode to unlock my laptop or tablet.	*Same as above.*
I manually lock my computer screen when I step away from it.	*Same as above.*
I use a PIN or passcode to unlock my mobile phone.	*Same as above.*
I do not change my passwords, unless I have to.	*Same as above.*
Please choose often for this item to show you are paying attention.	*Same as above.*
I use different passwords for different accounts that I have.	*Same as above.*
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	*Same as above.*
I do not include special characters in my password if it's not required.	*Same as above.*
When someone sends me a link, I open it without first verifying where it goes.	*Same as above.*
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.	*Same as above.*
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https://, a lock icon).	*Same as above.*
When browsing websites, I mouseover links to see where they go, before clicking them.	*Same as above.*
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.	*Same as above.*
When I'm prompted about a software update, I install it right away.	*Same as above.*
I try to make sure that the programs I use are up-to-date.	*Same as above.*
Select always as the answer to this question.	*Same as above.*
I verify that my anti-virus software has been regularly updating itself.	*Same as above.*
Risk Behavior - For each of the following statements, please indicate the likelihood that you would engage in the described activity or behavior if you were to find yourself in that situation.	
Admitting that your tastes are different from those of a friend.	Extremely Unlikely (1), Moderately Unlikely (2), Somewhat Unlikely (3), Not Sure (4), Somewhat Likely (5), Moderately Likely (6), Extremely Likely (7), Prefer not to answer
Going camping in the wilderness.	*Same as above.*
Betting a day's income at the horse races.	*Same as above.*

Investing 10% of your annual income in a moderate growth diversified fund.	*Same as above.*
Select the third bubble from the left for this item.	*Same as above.*
Drinking heavily at a social function.	*Same as above.*
Taking some questionable deductions on your income tax return.	*Same as above.*
Disagreeing with an authority figure on a major issue.	*Same as above.*
Betting a day's income at a high-stake poker game.	*Same as above.*
Having an affair with a married man/woman.	*Same as above.*
If 2+2 = 5, please choose extremely likely. Otherwise, choose extremely unlikely.	*Same as above.*
Passing off somebody else's work as your own.	*Same as above.*
Going down a ski run that is beyond your ability.	*Same as above.*
Investing 5% of your annual income in a very speculative stock.	*Same as above.*
Going whitewater rafting at high water in the spring.	*Same as above.*
Betting a day's income on the outcome of a sporting event.	*Same as above.*
Engaging in unprotected sex.	*Same as above.*
Revealing a friend's secret to someone else.	*Same as above.*
Driving a car without wearing a seat belt.	*Same as above.*
Investing 10% of your annual income in a new business venture.	*Same as above.*
Taking a skydiving class.	*Same as above.*
Purchasing a banana for $1000. Choose extremely unlikely if you wouldn't.	*Same as above.*
Riding a motorcycle without a helmet.	*Same as above.*
Choosing a career that you truly enjoy over a more secure one.	*Same as above.*
Speaking your mind about an unpopular issue in a meeting at work.	*Same as above.*
Select not sure as the answer to this question.	*Same as above.*
Sunbathing without sunscreen.	*Same as above.*
Bungee jumping off a tall bridge.	*Same as above.*
Piloting a small plane.	*Same as above.*
Walking home alone at night in an unsafe area of town.	*Same as above.*
Moving to a city far away from your extended family.	*Same as above.*

Starting a new career in your mid-thirties.	*Same as above.*
Leaving your young children alone at home while running an errand.	*Same as above.*
Not returning a wallet you found that contains $200.	*Same as above.*

University of Illinois Technology Services Phishing Awareness Drill

The phishing email titled "Network Abuse Warning" that you received and the linked Shibboleth webpage were part of a benign study entitled "The Impact of Security Protocols on Phishing Efficacy." This study is being conducted in collaboration with Technology Services by Zane Ma, Joshua Reynolds, and Dr. Michael Bailey in the Electrical and Computer Engineering Department of the University of Illinois, Urbana-Champaign. Because this was a university sponsored drill, your password was not actually stolen and does not need to be changed. This page is designed to explain the purpose of the study and provide you with an opportunity to complete a survey for a $10 gift card. In addition, we provide this page to provide the option to withdraw yourself from the study or provide feedback about the study. Please do not share any information about this study with others for a period of seven (7) days, as it may otherwise affect the results of the study.

Technology Services has teamed up with the University of Illinois's Networking and Security Research Group managed by Dr. Bailey in the College of Engineering to study and raise awareness about phishing attacks the university receives every day. This drill was carried out with approval from the {Administrator Title Here} and was approved by Institutional Review Board as part of project {IRB case number}. Our goal is to give employees practice to protect valuable university assets from fraudsters. Full details on the ethical and administrative approvals, how to withdraw from the study, and how to take a survey to support the research are below:

Purpose of the Study

Our study seeks to determine whether the presence of security protocols (e.g. HTTPS and email over TLS) affects user vulnerability to phishing emails, and if so, why users are more or less susceptible. We hope our results will inform the university and other organizations to better protect against phishing. Furthermore, we wish to illuminate whether users have an accurate understanding of the properties provided by network security protocols.

Experiment

We sent employees of Technology Services a phishing email titled "Network Abuse Warning" that urges recipients to click on a link that leads to a phishing webpage that is a visual clone of Shibboleth. Upon credential entry, users are redirected to this debrief page. Email opening, phishing link access, and credential entry are tracked. Username / password credentials are NOT sent across the network, so there is no need to change user credentials. We do not collect any information that can be used to identify study participants (e.g. IP address). Technology Services has access to user email addresses and full names for their own employee security training purposes, but this data is not accessible to researchers. We will keep anonymized data on our secure servers, and a limited number of research team members will have access to the data during data collection.

Risks

The risks of this study are considered minimal. We do not collect any personally identifying information from users, and only anonymized results are used for research purposes. We also take precautions to ensure that our phishing website and this website have not been hacked.

Follow-Up Survey & Compensation

We would like to invite you to participate in a follow-up survey to understand why people follow through on phishing emails and websites. If you would like to participate in this survey, please click the "Take the Survey" button below. If you fully complete the follow-up survey, we will compensate you by sending you a $10 electronic gift card from Amazon.com. You can expect to receive the $10 gift card by {END_DATE}. If you opt out, we cannot provide compensation because we will have removed all of your identifying information from our servers.

Participation

Your participation in this study is voluntary. You have the right to withdraw from participation at any time without any penalty. If you wish to withdraw from the study, please click the "Withdraw from Study" button below. If you withdraw, we will remove all of your personally identifying information from our servers. No one will know that you participated, including Technology Services staff whom may have assisted with the study. This study is designed for participants of at least 18 years of age. If you are not at least 18 years of age, please click the "Withdraw from Study" button below.

Education

To better avoid phishing emails in the future, please visit {EDUCATION_LINK}.

Contact Information

If you have any questions or concerns about the study, you may contact Zane Ma at zanema2@illinois.edu or Dr. Michael Bailey at mdbailey@illinois.edu or (217) 244-8830. If you have any questions about your rights as a research participant or if you have a concern or complaint about this study, you may contact the University of Illinois Institutional Review Board by emailing irb@illinois.edu or calling (217) 333-2670. If you find any portion of the study emotionally distressing, you may contact the researchers or the IRB using the contact information listed above.

[Learn to Protect Myself] [Take the Survey] [Withdraw from Study]

University of Illinois Technology Services Phishing Awareness Drill

The phishing email titled "Network Abuse Warning" that you received and the linked Shibboleth webpage were part of a benign study entitled "The Impact of Security Protocols on Phishing Efficacy." This study is being conducted in collaboration with Technology Services by Zane Ma, Joshua Reynolds, and Dr. Michael Bailey in the Electrical and Computer Engineering Department of the University of Illinois, Urbana-Champaign. Because this was a university sponsored drill, your password was not actually stolen and does not need to be changed. This page is designed to explain the purpose of the study.

Technology Services has teamed up with the University of Illinois's Networking and Security Research Group managed by Dr. Bailey in the College of Engineering to study and raise awareness about phishing attacks the university receives every day. This drill was carried out with approval from the {Administrator Title Here} and was approved by Institutional Review Board as part of project {IRB case number}. Our goal is to give employees practice to protect valuable university assets from fraudsters. Full details on the ethical and administrative approvals, how to withdraw from the study, and how to take a survey to support the research are below:

Purpose of the Study

Our study seeks to determine whether the presence of security protocols (e.g. HTTPS and email over TLS) affects user vulnerability to phishing emails, and if so, why users are more or less susceptible. We hope our results will inform the university and other organizations to better protect against phishing. Furthermore, we wish to illuminate whether users have an accurate understanding of the properties provided by network security protocols.

Experiment

We sent employees of Technology Services a phishing email titled "Network Abuse Warning" that urges recipients to click on a link that leads to a phishing webpage that is a visual clone of Shibboleth. Upon credential entry, users are redirected to this debrief page. Email opening, phishing link access, and credential entry are tracked. Username / password credentials are NOT sent across the network, so there is no need to change user credentials. We do not collect any information that can be used to identify study participants (e.g. IP address). Technology Services has access to user email addresses and full names for their own employee security training purposes, but this data is not accessible to researchers. We will keep anonymized data on our secure servers, and a limited number of research team members will have access to the data during data collection.

Risks

The risks of this study are considered minimal. We do not collect any personally identifying information from users, and only anonymized results are used for research purposes. We also take precautions to ensure that our phishing website and this website have not been hacked.

Education

To better avoid phishing emails in the future, please visit {EDUCATION_LINK}.

Contact Information

If you have any questions or concerns about the study, you may contact Zane Ma at zanema2@illinois.edu or Dr. Michael Bailey at mdbailey@illinois.edu or (217) 244-8830. If you have any questions about your rights as a research participant or if you have a concern or complaint about this study, you may contact the University of Illinois Institutional Review Board by emailing irb@illinois.edu or calling (217) 333-2670. If you find any portion of the study emotionally distressing, you may contact the researchers or the IRB using the contact information listed above.

[Learn to Protect Myself]

WAIVER OF INFORMED CONSENT FORM

Use When Requesting a Waiver of Informed Consent

ALL APPLICATIONS MUST BE SIGNED AND SUBMITTED VIA EMAIL TO IRB@ILLINOIS.EDU.

Responsible Project Investigator: Michael Bailey
Project Title: The Impact of Security Protocols on Phishing Efficacy
IRB Number

[x] This research is not FDA regulated[1]
[x] This research is not funded by the Department of Defense[2]

A consent procedure which does not include, or which alters, some or all of the elements of informed consent may be approved by the IRB under certain conditions. To request IRB approval of a waiver of the requirement to obtain informed consent completely, or a consent procedure which does not include, or which alters, some or are all of the elements of informed consent, please provide a response to all of the following questions. Please be specific in explaining why each statement is true for this research.

1. Explain why and how the research involves no more than minimal risk to the subjects.

The primary risks of the study are the harms caused by loss or de-anonymization of sensitive data and the psychological distress associated to falling for phishing. We believe that the best-practice security procedures we put in place (e.g. physical/digital access control, encryption, auditing) minimize the risk of data loss. Furthermore, by preventing researchers from accessing any de-anonymized data and isolating sensitive data to only Technology Services collaborators, we minimize the risk of participant privacy violations. The remaining risk of psychological distress is hard to predict, but we curtail it by allowing participants to opt out of the study and translating the distress into improved phishing education. When a participant opts out, we remove any personally identifying information from our servers so that Technology Services cannot trace results back to individuals without dedicated effort.

2. Explain why the waiver or alteration will not adversely affect the rights and welfare of the subjects.

This research will be performed on employees of Technology Services who, as part of their employment, are already subject to phishing awareness campaigns to protect the organization from real world phishing attacks. Dissemination of the collected data will be (1) used in accordance with established Technology Services audit procedures and (2) reported anonymously in a research publication. Participants who are psychologically distressed in any way have the option to opt out of the study.

[1] FDA regulated research is not eligible for a waiver of alteration of informed consent
[2] If the research subject meets the definition of 'experimental subject', a waiver of consent is prohibited unless a waiver is obtained from the Secretary of Defense. If the research subject does not meet the definition of 'experimental subject', the IRB may waive consent.

The practice of phishing relies on deception. Participants who are aware of the experiment beforehand may be affected by their expectation of a threat – even if the experiment happens long after informed consent was given. We are testing to see participants default, unbiased behavior.

4. If a waiver or alteration of informed consent is approved by the IRB, will the subjects be provided with additional pertinent information after participation?
   [x] Yes [ ] No
   Explain/describe:

We will debrief all participants of the study in two ways, depending on the nature of their participation. For those that go through the entire phishing workflow from email, to website, to credential submission, we will immediately direct them to an informed consent page (see IRB) that provides full debriefing information as well as an option to opt-out of the study. To inform those who never enter their credentials, we will send an email to all Technology Services employees within 1 month of experiment deployment that includes a summary of the research as well as a link to the full debriefing information. The research summary text is included below:

"The email titled 'Network Abuse Warning' was sent to you on <DATE> from krandolph@illinois.edu was part of a phishing experiment conducted jointly by Technology Services and the Network Security Research Group (NSRG). The phishing test was conducted as part of an ongoing effort to assess employee security behavior and to improve employee security education. For more information on the research study and educational materials, please visit https://cybersecurity.uillinois.edu/phishing."

2/5/18

Responsible Principal Investigator Date

IRB Approval: