Filet-o-Phishing our Friends

Thanya Nguyen, *CS569* Dylan Sullenberger, *CS569*
Cam Witt, *CS469*

Abstract

Phishing continues to be a cybersecurity threat that preys on individuals' trust and lack of vigilance. This project explores phishing susceptibility among college students and faculty by creating a mock website that mimics a familiar university platform, Canvas. Using this fake website, we conducted a controlled phishing experiment targeting both computer science (CS) and non-CS students to examine their likelihood of falling victim to such attacks. Participants were informed of the phishing attempt and guided to a survey to provide feedback, ensuring no sensitive information was stored. Results revealed significant differences in susceptibility, with non-CS students being 11 times more likely to submit personal information compared to CS students. Factors such as familiarity with phishing, critical evaluation of URLs, and browser warnings influenced participants' behavior. The findings underscore the importance of cybersecurity education and awareness, highlighting potential strategies for mitigating phishing risks in diverse student populations. This research contributes to understanding human vulnerabilities in cybersecurity and offers insights for improving phishing prevention.

1. Introduction/Motivation

Phishing remains a prevalent cyber threat, exploiting human psychology to steal victims' information. Understanding why individuals fall for these scams is essential for improving prevention. Our research aims to explore this by consensually testing college students and faculty through a mock website mimicking familiar platforms like Canvas, VolPrint, or MyUTK. We will track who clicks the link and submits their credentials, without storing their information, and then inform them of the phishing attempt to raise awareness. This study will compare the susceptibility of computer science students, who are more familiar with phishing, to that of students from other disciplines, helping us understand and prevent future attacks.

The first question we are attempting to answer is how much a background in computer science and cybersecurity has on susceptibility to phishing attacks. Our hypothesis for this is that when we test against computer science vs. non-computer science students that hopefully the computer science students are less susceptible for being phished because they have more cybersecurity awareness than non-computer science students that don't have to learn about this every day in class. We expect that the non-computer science students are more likely to click on the link and submit their personal information because they are not constantly aware of the issues of phishing attacks as much as computer science students, who have more of a background in computers and basic security concepts as part of their curriculum.

We are also attempting to see whether or not students are more likely to fall for phishing links when they are sent from friends. A fairly common way for links such as these to be spread is for one account to become compromised, and then the attacker uses this compromised account to attempt to phish people in the compromised account's contact list. We hypothesize that users will be more likely to fall for phishing scams if they receive the link from a friend's account.

Additionally, we will perform qualitative analysis on the reasons that people do or do not fall for phishing attacks. We will conduct a survey asking the reasons users do or do not fall for attacks and see if any common trends appear for either question. This could help better understand why people fall for phishing attacks and what methods best help to protect against them. This data can then potentially be utilized to help direct anti-phishing awareness and education in the future, both in terms of instructing people of what to look for and how to effectively avoid it.

2. Related Work

When searching up information on related work, there are YouTube videos and GitHub repositories that have almost everything we need for this. There are YouTube videos such as, "Phishing attacks are SCARY easy to do!! (let me show you)" which goes step-by-step on how to create a fake website from the repository and show how the program can be ran to harvest the data. This "Blackeye" repository found on GitHub can be used to create some premade websites like LinkedIn or Instagram. We may use this as inspiration on how to harvest the data, but we will be constructing the website ourselves.

3. Methods

Our experiment was conducted in multiple phases. The first phase consisted of building our phishing website, which involved acquiring the domain, ripping the code from the normal Canvas log-in page, and editing this code in order to ensure that the website does not save any sensitive information and instead redirects users to the survey page that we needed it to redirect to. The second phase was where we phished our friends, which consisted of sending out the phishing website to people and recording their responses.

Acquiring the domain was fairly simple. We looked at websites selling domains, looking for a URL that would be a believable URL for the log-in page for Canvas at the University of Tennessee. We settled on *canvas-tennessee.org*. This domain cost us about $15 to purchase for a whole year, and the three of us split this cost evenly. We hosted the website through GitHub, and the repository for our ewbsite can be found at https://github.com/thanyalasagna/cosc569-fop.

After the domain had been acquired, we began work on building the website. The first step was to rip the code from the normal log-in page for Canvas. This was quite difficult at first. However, using tools with node.js, we were eventually able to rip the HTML, CSS, and JavaScript in a way that appeared to be very convincing.

Before deploying the website, we needed to edit the functionality. At first, it would attempt to log users in and redirect them to the DUO two-factor authentication page, which clearly would not have worked since our website was not the real Canvas log-in. The main change we needed to make was to rework the log-in button such that, when pressed, it would not attempt to log users in in any way and would instead redirect them to a Google form (where we were hosting our survey). This was fairly simple, and just involved editing a few lines of the HTML and JavaScript. There will be more details on the survey in section 4.

Initially, we had planned for our website to have functionality to store user's NetIDs (not passwords) locally, in order to ensure that they were filling out the form accurately. However, we eventually decided against doing this for ethical reasons (especially after our website started unexpectedly showing up on search engines). Our fake phishing website did not store any personal information from any user.

After the process of building and testing the website to ensure everything was working how we wanted it to had been completed, we began sending it out to our peers. Each team member compiled a list of 10 computer science majors and 10 non-computer science majors to whom the link would be sent. When sending it out, we added a few fake parameters in order to try to distract users from the incorrect domain name. The users in question were sent the following message:

Hey can you fill out this survey to help me with a class project? I need more responses to meet the goal: https://canvas-tennessee.org/?surveyid=c3VydmV5IGZvciBodW1hbiBmYWN0b3JzIGluIGN5YmVyc2VjdXJpdHk&refurl=dWggb2ggc3BhZ2hldHRpIG9z&projectid=Y29vbCBzdXJ2ZXksIHdvdWxkIGRlZmluaXRlbHkgdGFrZSBpdCBhZ2FpbiBpZiBpIGhhZCB0aGUgY2hhbmNl

The message did let users know that they were helping out with our project, albeit not in the way they would have expected to. 60 students in total were sent this message. 20 were sent the message through email, and 40 were sent the email over Discord. Half of these students were Computer Science majors, and the other half were non-Computer Science majors.

If students responded to our message saying that they could tell it was fake, or that their browser or internet provider blocked the website due to suspected malicious activity, we would send them a direct link to the Google form so they could still fill out the survey, as the data and feedback that these students would be able to provide would still be extremely valuable to our study.

Additionally, many students found our website by accident via search engines such as Google, Bing, DuckDuckGo, etc. This was very unexpected, and we had not accounted for this possibility in the initial version of our survey. This actually first started happening before we had sent out our message to our peers. In order to account for this unexpected circumstance, the survey was modified, and we added an additional question in the survey to ask whether they had received the link from us or found it via search engine, and if they had found it via search engine, we added a question asking which search engine in particular they were using.

4. Complete Survey/ Interview Questions

Upon clicking the login button on the phishing website we have created, our targets will be redirected to a survey which was hosted on Google forms. The survey opens by telling victims at the top of the page that they have been phished and assuring them that we have not saved their personal or sensitive information. This is listed in larger font and bolded to ensure that users are aware that none of their information was saved anywhere. The survey explains that the website they visited was part of a phishing awareness project and tells them to fill out the form to help us gather data. It also links to a resource with phishing awareness and safety tips.

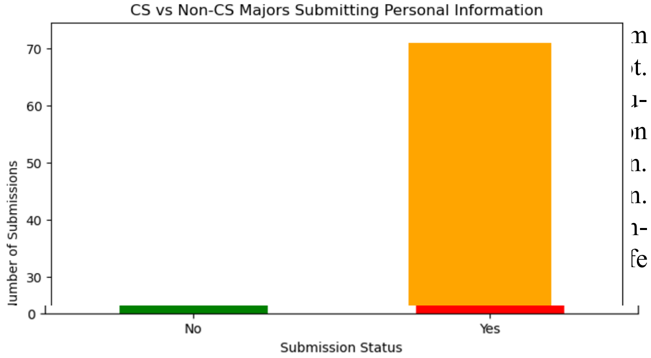
The survey asks the following questions: what year in school the victims are (freshman, sophomore, etc.), what their major is (computer science or non-computer science), how they got to the website (search engine, email, Discord, etc.), which search engine they found it through (if found through search engine; Google, Bing, DuckDuckGo, etc.), which project member sent them the link (if they were sent it by one of us), was sensitive information submitted, and what factors led them to submit or not submit personal information.

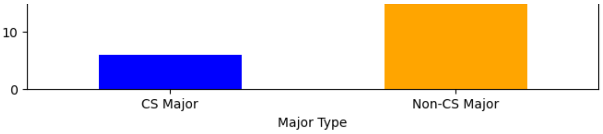
The questions of what year, major, method of finding the website, and whether personal information was submitted were multiple choice questions, which allowed us to do quantitative analysis on the impact of year and major on the effectiveness of phishing websites, as well as whether they are more likely to fall for phishing attacks when the link is sent from a friend. The question of the factors that led them to submit or not submit personal information, by contrast, was an open-ended short answer question, which allowed us to do more qualitative analysis on why certain groups of students do or don't fall for phishing websites.

5. Results

The results show that there are 100+ submissions in the Google Form. This number of submissions continues to slowly grow as the semester progresses. There are some submissions that are not presented in the following graphs due to random UTK students who have been phished by this website after the production of these graphs. There are 15 computer science majors that have been recorded with 94 non-computer science majors recorded as well.

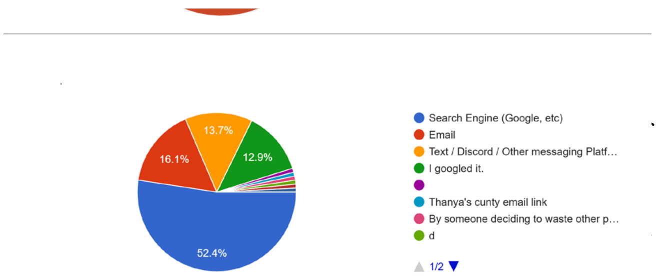
The graph above shows that overall, 77 students submitted personal credentials while 32 students did not.





Graph of CS vs non-CS students who submitted personal information.

Subjects who filled out the survey range from many different grade levels. The grade level with the most submission is seniors at 33.8%, followed by 23.1% of juniors, 20% sophomores, 15.4% freshman, 6.9% graduate students and <1% faculty.



When asked which website search engine they used, 63.6% accessed this through Google, followed by 9.1% from Bing. The number of subjects who answered this question is 73, which is less than other questions due to not all of them finding this from a search engine.

When asked "What factors led you to submit/not submit your information? Anything you would like to tell us?" 127 responses were recorded with a good number of those responses being blank answers. After passing through the responses, the following table shows some responses of the CS majors who didn't submit personal information:

CS majors who didn't submit personal information
"Safari warned me that it was a scam!!! Thank you Steve Jobs."
"erm the url was sus and my password manager didn't automatically fill in my username and password"
"The domain didn't resolve to the proper UTK domain, so I punched it into who.is and it said the domain was registered in September. The real canvas domain was registered in 1999, and UTK's domains all have special EDU WHOIS info."

This shows that the computer science students used their knowledge learned from school and were able to apply those skills to this scenario and avoid submitting their personal information. Some students CS/non-CS did not submit personal information due to autofill not filling the fields when they should've.

For non-CS majors who didn't submit personal information, many of the responses were blank or said, "nothing" however some of the notable responses are the following:

Non-CS majors who didn't submit personal information
" I have absolutely no idea what this is. All I did was search for canvas on google so I can print a paper. This is super annoying and is taking up my precious time for just clicking on canvas."
"I noticed that my usual self-login ID didn't work so I expected that something was amiss. "
"im trying to study"

On the other hand, there were many more responses of subjects who submitted personal information. Specifically for non-CS majors, some of the responses reveal that they were truly phished by their friends or were in a hurry to finish an upcoming assignment. These results also gave our team a discovery that subjects believed the website was real because there was Duo Push Factor Authentication applied. The subjects thought the Duo Push notification was to verify their sign-in to Canvas, however the notification was for sign-in for access to the Google Form.

Non-CS majors who did submit personal information
"Link follows the usual UTK qualtrics procedures (i.e. having to log in, and I'm always logged off on my phone), surveys are pretty common for classes"
"It was my friend 😭 and I had to use DUO 2FA and everything to get to the form, so I thought it was safe. Should have known better 🙂↔"
"What just happened lol. I rented a computer from the library, and typed in utk canvas login. Then I submitted my stuff to login and wound up here. You got me, lol."
"I need to take an exam"

Lastly, for the CS students that submitted personal information, some of the responses were due to the team project spear phishing the student, but other responses were due to falling for a convincing website.

CS majors who did submit personal information
"The login looked official (UT logo and whatnot) so I trusted it. And I didn't think thanya would phish me"
"it looked legit and was sent to my by a friend"
"I'm in a group with Cam in a Computer Science class and they listed a professor at the school and that it's for cybersecurity."
"If it had not been for those three factors I would have stopped when my username and password didn't auto-populate for the form submission."

While all these responses were insightful as to how subjects were able to stumble to this website and voluntarily fill out the form, some of the responses were funny or borderline inappropriate. These responses seemed fueled from anger or frustration from accidentally clicking on this link multiple times. Students were in a rush to get logged into Canvas and did not think twice about the website they were clicking on. Many students stumbled onto this website through the public computers in the library too. Some of the unusual, yet worth mentioning responses were:

Honorable Mentions
“PLEASEEEE DONT TAKE MY PASSWORD PLEASEEEEEEEEEEEEEEEEEEEEEE OHMYGAHHHHHHH YALL GOT MEEEEEE IM SORRY PLEASEEEEEEEEEE”
“because it looked exactly like the utk login, how the hell was i supposed to know assholes”
“BRO why does this keep popping up every time I log into canvas “
“I was held at gunpoint”
“felt pretty real good work gang”

Other responses that were not insightful to further research, but still worth mentioning.

After looking at these responses, we can gather that there are many different reasons as to why students would stumble on this phishing website and submit their information. There were not as many CS students that submitted personal information and even less CS students that filled out the form compared to non-CS students.

6. Challenges and Limitations

The first challenge we faced in this project was properly cloning the look of the Canvas login page. We wanted to make sure that our website looked as closely to the real one as possible. To accomplish this, we implemented a Node.js script that cloned the website, including the styling and scripting. A Node.js library called “website-scraper" was useful for this, as it made cloning the entire page source extremely easy. With this, we were easily able to replicate the real login page exactly in terms of appearance.

We temporarily faced the challenge of HTTPS certification. Our website did not possess the proper certification, so connections to our website caused the user to see a warning for our site being “not secure”. In time, this was resolved, and visitors to our website no longer saw this warning.

The next challenge we faced was creating an inconspicuous URL to send to our targets for them to click. We ended up purchasing a domain name that seemed plausibly real. In addition to this custom domain, we added parameters to the URL we sent our targets. This made the link much longer, which seemed to help our targets miss the fact that the link they were clicking was not of the proper domain.

Our website was flagged as a phishing website by some service providers’ anti-spam systems. As a result, our website would be blocked on certain networks, displaying a warning to the user that the website was fraudulent, or preventing the user from accessing the page entirely. Fortunately, none of these networks were that of the university, so we were still able to phish those on the UTK network.

Another unexpected challenge we have faced is that users were able to find our website via search engines, which we had not initially planned for. It appears our website came up very high in Bing’s search algorithm when searching for “canvas tennessee” or similar terms, which causes our website to come up very high when students search for Canvas via Bing or DuckDuckGo. In some cases, it comes up earlier than the actual Canvas login. Due to this unforeseen issue, we had to edit the survey, and scrap features we had initially planned for the website to avoid ethical issues. This did, however, take care of the initial challenge we were concerned about, which was whether or not the website would be convincing enough to actually phish people.

After our phishing was complete and our data collected, we still faced the issue of sorting through incorrect survey responses. Because our survey was only available to those with Google accounts within the university, some subjects interpreted the Google login for the survey as the login for our website, which caused them to submit incorrect responses to our survey. Luckily, this data was able to be corrected by going through our responses and reading the other data submitted.

The main limitation of this study was the constrained demographic to which our attack was available. We planned initially to only target our friends, but the appearance of our website on search engines enabled us to quickly expand who we could target. Despite this, our attack only applies to those at the University of Tennessee in Knoxville.

7. Lessons Learned / Future Work

Our lesson that we learned from initial study is that there was trouble getting the domain correctly linked to the fake website. We learned that it was a little harder than we thought it would be. However, while it was harder than we expected it would be initially, it was still a lot easier to create and host a phishing website than it really should be.

We had also learned that there was an issue that our website got flagged for phishing, however we have been granted the infamous green padlock which signifies to the non-computer science student that our website is safe and HTTPS encrypted.

Another website learned is that it is shockingly easy to get phishing websites high on search results. Our website showed up on many different search engines, and on some (in particular, Bing and DuckDuckGo), it was as high as the second search result from the top when searching for "canvas tennessee" or "canvas utk". We initially were not expecting anybody to find our website through search engines, and as such, we had not originally included anything in our survey to account for people accessing the website through search engines. However, it is much easier than one would expect it to be to show up very high in the algorithms used by search engines.

As such, it is likely better for users to doublecheck the URL of whatever they are clicking on on Google before going there. For Canvas specifically, students should probably access it through the official channels (or by bookmarking the site) instead of by Googling it. Our website was harmless, for research, and did not store any of users' personal information, but if it was this easy for us to show up high on search engines, it wouldn't be hard for malicious websites to do so either.

UTK also needs to increase its anti-phishing awareness, especially for students who do not have as much of a background in computer science or cybersecurity. There were much more non-computer science majors who submitted personal information compared to computer science majors, and some of them left comments suggesting that they did not even know what phishing was or that they had no way of knowing that our website was fake. This indicates that the university does not provide good resources for making users aware of how to avoid phishing attacks.

It is worth noting that computer science majors did a much better job at avoiding submitting personal information, with only 6 computer science majors saying they submitted personal information. 9 said that they did not submit personal information, but what is even more telling is that we specifically sent out 30 links to computer science majors. This means that at least 15 computer science majors saw the link and either ignored it, or clicked on the website and did not click the log-in button (and never messaged us to let us know). This suggests that computer science majors are better at avoiding phishing attacks compared to non-computer science majors, and while improvements to the anti-phishing awareness within the field at UTK could still be improved, it is in a much better state than that of the non-computer science majors.

There are a few areas of potential future work that could be done. First, a test could be done that involves the faculty more. Only one faculty member was sent the link as part of our initial study. As there are a large number of faculty members at the university, it is a significant demographic and more research should be done to ensure that they are getting the anti-phishing awareness training that they need to be getting.

Additionally, everyone links were sent out to were our friends. Students that we did not know found the website via search engines, but none were emailed the link or sent the link via Discord. As such, the experiment could be modified to have the participants selected more randomly. This could minimize the bias. A possible way that this could be conducted would be to have half of the recipients be friends of the team doing the study, while the other half could be chosen at random from a list of active students at the university. Having an equal number of both groups would be able to show more accurately whether or not students are more likely to click links when they are received from a friend.

Another way the study could be improved upon is to even out the number of each grade level receiving the link. Having an equal number of freshmen, sophomores, juniors, seniors and graduate students would make it so more definitive conclusions could be drawn on the relationship between time in school and awareness of phishing attacks and how to avoid them.

Lastly, similar experiments could be ran at other universities. This could test the effectiveness of phishing websites and of anti-phishing awareness at other universities, and it would be possible to draw comparisons between phishing awareness at UTK compared to other universities.

8. Discussion/Conclusion

For the question of whether computer science or non-computer science majors are more susceptible to phishing attacks, our study suggests that non-computer science majors are much more susceptible to this kind of attack. Approximately 75.5% of non-computer science majors who filled out the survey indicated that they had submitted sensitive information. By comparison, only 40% of computer science majors who filled out the survey had submitted sensitive information. This drastic difference in percentages alone would indicate that non-computer science majors were more susceptible to phishing attacks.

However, what is arguably more telling is the unrecorded subset of users who were sent the link and/or came across the link on search engines and did not click on it or fill out the survey. While we have no way of measuring just how many students came across the link via search engines, we do know that 30 computer science majors and 30 non-computer science majors were sent the link by group members. Only 15 computer science majors filled out the form. This indicates that at least half of the computer science majors who were sent the form by a team member did not submit data and never indicated to us that they had clicked the link in the first place (and, as such, would never have received the survey link). And as we know that the website was appearing on search engines, we can almost assure that computer science majors likely came across the link via search engines as well, but still went to the website at a much lower rate. By comparison, 94 survey takers indicated that they were non-computer science majors. As such, due to the data of both the percentages of survey takers that submitted personal information and also due to the difference in number of survey takers, we can conclude that non-computer science majors are more susceptible to phishing attacks than computer science majors. This is consistent with our hypothesis, and makes sense since computer science majors would have had much more awareness to phishing attacks built into their curriculum.

Regarding the affect of the year of school that students are on how susceptible they are to phishing attacks, no strong concolusions can be drawn. The highest number of people that filled out the form happened to be seniors, followed by juniors, then sophomores and then freshman, which could suggest a direct correlation between how long students have been attending and how likely they are to fall for phishing attacks. However, as the group members were made up of majority seniors, it is more likely that more of their peers were seniors, which would also suggest that more seniors were sent the survey link than other grades. This seems to be a much more likely cause of this apparent correlation. As such, with that bias in mind, it is hard to draw any definitive conclusions from this data point. Additionally, common sense would suggest that those who have been in school longer would be more aware of phishing attacks, not less aware of them.

For the question of whether or not people are more likely to fall for attacks when sent them presumably by a friend, the data is also somewhat inconclusive. We do know that more people came across the website via search engine than via links from group members. However, without the data of exactly how many people saw the website on search engines such as Google, Bing, or DuckDuckGo, we cannot determine a percentage of users that clicked on the link from search engines compared to those that did not. This lack of a specific percentage makes it very hard to accurately compare the likelihood of a student falling for a phishing link when sent the link by a friend against the likelihood of the same student falling for a phishing scam they came across in the wild. For a future study, one could separate a group of people to send the links to randomly from a list of students, as this would lead to a more controlled number and make it easier to draw conclusions in this area. But for now, with the data we have available to us, no strong conclusions can be drawn in this area.

For users who chose not to submit personal information, there were many reasons that survey participants said for why they did not. One of the most common reasons people listed as to why they did not submit personal information were that their password managers did not autofill their passwords Another very common reason was that their browser/internet provider warned them about the site Finally, a third common reason was that they deduced from the domain that it was fake. These indicate awareness from these users of phishing techniques and how to avoid them, and/or discipline to follow warning signs that their technology indicates for them. The practices employed by these users align with good practices to avoid being phished, and these practices could be implemented into anti-phishing awareness education to keep more students from falling for phishing scams such as the one conducted in this study.

In contrast, a lot of users who did not submit personal information either did so because they did not know what was going on or because they were sent the link by a friend, and thus assumed the link was safe to click. The group of users that did not know what was going on, either because they thought the link looked harmless because they did not know what warning signs they should be looking for, or because they were in a rush for one reason or another, indicates a severe and alarming lack of anti-phishing awareness. These responses suggest that better education should be put in place to increase students' awareness of common phishing techniques. The latter group of response, who submitted personal information because they were sent the link by a friend, suggests that, if sent the link someone that they trust, students will sometimes avoid their usual awareness and trust the friend, when this cannot be assumed to always be the case. Sometimes, the friend's account could be compromised, and the attacker that has access to the friend's account could be acting maliciously to try to get access to more accounts. This is a fairly common phishing tactic, and has been employed over email and Discord (just like our experiment). As such, users should always stay aware of potential phishing attacks, and they should not let their guard down just because a link is sent to them by a friend. This knowledge should also be covered in anti-phishing awareness education.

To summarize, in this paper, we have conducted a study to measure the efficacy of the University of Tennessee-Knoxville student body's phishing awareness. We created a phishing website modeled after the Canvas log-in page, had it redirect to a survey where we asked demographic questions and questions about if and why they submitted personal information, and sent the link to a total of 60 of our peers. We also received submissions from users who found the link via search engines. We were able to conclude that non-computer science majors are much more susceptible to phishing attacks than computer science majors. We also suggest that anti-phishing awareness and education need to be increased across the whole student body, especially in the case of non-computer science majors who do not come into contact with cybersecurity concepts and phishing awareness as a norrmal part of their curriculum. Finally, we recommend that this education should include recommending the use of tools such as password managers, as well as encouraging discipline to heed warnings that are provided by the browser or internet provider. As this was a simple, baseline study, further research should be conducted in order to gain further demographic results and insight onto the factors that lead students to fall victim to phishing attacks. Thank you so much for reading.

9. Sources

"Phishing Attacks Are SCARY Easy to Do!! (Let Me Show You!) // FREE Security+ // EP 2." YouTube, NetworkChuck, 28 Oct. 2020, www.youtube.com/watch?v=u9dBGWVwMMA&t=60s&ab_channel=NetworkChuck.

Poel, Erickson Hyppolite. "Ericksonathome/Blackeye: BLACKEYE v2.0: New Phishing Tool with Localtunnel." GitHub, 23 Aug. 2024, github.com/EricksonAtHome/blackeye.

10. Appendix A – Contents of Our Survey

Pre-survey Disclaimer:

"Your sensitive information is not saved for this project. We did not collect any of your login credentials!

The website you visited is part of a phishing awareness project by students at the University of Tennessee Knoxville. You just have been phished by UTK students in the Human Factors of Cybersecurity Research Project!

Please complete this form to explain to us how you got phished and what steps you did to get here.

[Here](https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams) are some phishing safety awareness resources, be careful out there!"

Survey Question 1:
"What year are you?"
- Freshman
- Sophomore
- Junior
- Senior
- Grad Student
- Faculty

Question 2:
"What is your major?"

Question 3:
"How did you get to this website?"
- Search Engine (Google, etc)
- Email
    - Text / Discord / Other messaging Platform
    - Other (fill in the blank)

Question 4:
"If you found this website through a search engine, which was it?"
    - Google
    - Bing
    - DuckDuckGo
    - Brave Search
    - Other (fill in the blank)

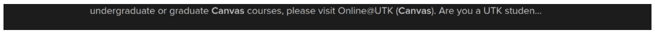
Question 5:
"If you were sent the link to this website by one of our project members, who was it?"

Question 6:
"Did you submit personal/sensitive information? (username/password)"
- Yes
- No

Question 7:

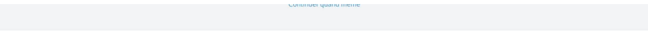
“What factors led you to submit/not submit your information? Anything you would like to tell us?”

11. Appendix B – Screenshot of the Website in Search Results



undergraduate or graduate **Canvas** courses, please visit Online@UTK (**Canvas**). Are you a UTK studen...

12. Appendix C – Screenshot of Safe Browsing Warning for Our Website



13. Appendix D – Screenshot of HTTPS Warning for Our Website

14. Appendix E – Disclaimer at the Beginning of Our Survey

15. Appendix F – Code used to Clone the Canvas Login Page