Project 3G, Report

CS321, Group 3
Sam Hutcherson, Chase Wallendorff, Justin Pirman, Jose Becerril

ScamSlam

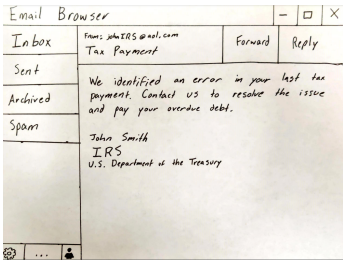
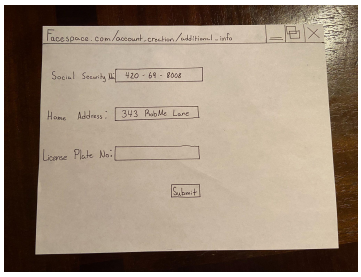
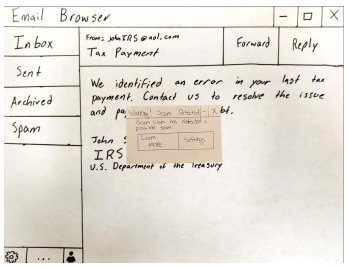
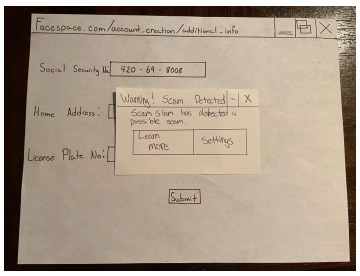
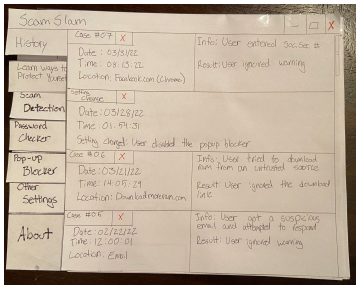
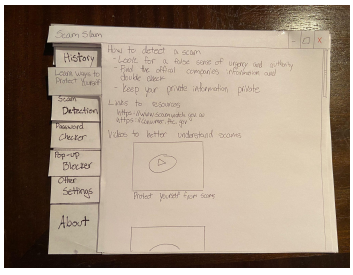
Team Members

Sam Hutcherson - Created and did initial formatting for the final report - helped to gather information for and finish several major sections of the document.
Justin Pirman - Added many of the photos and formatted them into the appendix and the prototype sections.
Jose Becerril - Helped to gather information for the final report and helped to finish several major sections of the document.
Chase Wallendorff - Handled the "problem and solution overview," "heuristic evaluation," and "discussion" sections.

Problem and Solution Overview

The problem our group has chosen to tackle is the issue of scams; this is a problem that millions of people encounter daily and that nobody - no matter how well educated or how aware of their situation they might be - is immune to. The scope of this problem is massive, ranging from technology based scams such as hacking, phishing, or viruses to more traditional types of scams such as fraud, impersonation, or price gouging. To combat the many and varied methods scammers use to do their work, we've designed a suite of anti-scam software, able to protect and keep the individual aware as well as educate them and help them live a more secure life.

Initial Paper Prototype: *Complete paper prototype shown in Appendix Figure 1*

<table>
<tr><th colspan="2">Task #1: Determining if a message is suspicious</th><th colspan="2">Task #2: Keeping Private Information Private</th></tr>
<tr><td>Frank received an email from who he thinks is the IRS. Frank didn't catch on that the email is from an untrusted account.</td><td> 
</td><td>Bob is trying to create a social media account, but stumbles into the wrong site.</td><td> 
</td></tr>
<tr><td>Our software detects that the email that Frank received was fraudulent and warns him about it. Frank clicks on the "Learn More" option.</td><td> 
</td><td>As Bob is entering his personal information, our software notifies him that the website is not trusted.</td><td> 
</td></tr>
<tr><td>ScamSlam opens the interface to the History tab. This shows all the scams that our software has detected. Frank then opens the Learn Ways to Protect Yourself tab.</td><td> 
</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Frank finds resources to prevent scams. He learns that the IRS does not email taxpayers and now doesn't even respond to emails from the IRS anymore.</td><td> 
</td></tr>
</table>

Pop-up Warning *Figure 1*

This is a warning given to the user to inform them that a scam has been detected. The pop-up is the most vital part of the entire software and can be changed with the settings in the UI itself.

History Tab *Figure 1*

Whenever the user selects the "Learn More" option on a pop-up as well as whenever the user starts up the interface, the software directs the user to the *History* tab. This tab stores each instance of the software detecting a scam even when the pop-up is disabled. The software also keeps track of the action taken by the user in addition to any relevant information about the scam including the time, date, location, and the reason the software was activated.

Learn Ways to Protect Yourself Tab *Figure 1*

Whenever the interface is open, the user can navigate through the different tabs using the menu located on the left hand side of the screen. This tab gives information that both our software and experts use to detect scams and teaches the user of ways to prevent them from becoming a scam victim.

Scam Detection Tab *Figure 1*

The *Scam Detection* tab gives the user the ability to set the scope of our software. The user can set if they want the program to not scan through their emails whenever viewing them. It should be noted that each option is enabled on default when installing our program. This is to ensure that less tech savvy users will be protected the moment they install the application.

Password Checker Tab *Figure 1*

The *Password Checker* tab has both settings in addition to a feedback section for user-entered passwords to check how strong they are. When enabling the "detection of passwords" option, our software automatically censors any instance of the user's saved passwords in the event that they send or post their password accidently. The user can also set the minimum security for passwords on websites, this prevents the user from making a password that would be considered weak even on sites that do not have any password requirements.

Pop-up Blocker Checker Tab *Figure 1*

The *Pop-up Blocker* tab is automatically enabled, but gives the user different settings that could be changed to whatever they would like. An option is available to disable the pop-up on certain sites if the user finds them annoying. Even if the user disables pop-ups, the software still records the data in the history but does not give a result on the user's actions.

Other Settings Tab *Figure 1*

The *Other Settings* tab gives various settings that only affect the interface itself. The user can change the color of the interface as well as the font and text size.

About Tab *Figure 1*

The *About* tab gives a brief summary of what we want from the program as well as any updates that could happen to the interface.

Testing Process

When testing the prototype, we received both Heuristic Evaluations of the paper prototype, and Usability tests.

Heuristic Evaluations were conducted by groups 8 and 10. For each group we gave them the paper prototype and watched them naturally interact with the UI. After they had gone through everything, they evaluated the prototype based on the Nielsen Heuristics.

Usability tests were done by three participants. For each participant, we had them interact with the scenarios given by our 2 tasks: determining if an email message is suspicious, and keeping private information private.

Our first participant was a 22 year old mechanical engineering student here at SIUE. He, like many other students here at SIUE, receives obvious email scams often. So he was interested to see our solution to address scam messages. We gave him the first task, and watched him interact with the paper prototype while commenting on what he thought about the usability of each tool. After he was finished, we received plenty of feedback and revised the paper prototype for our next participant.

Our second participant was a 23 year old computer science major at SIUE. He also met and ran through the 2 tasks on the paper prototype, while critiquing any usability issues, or problems with the changes that we made to the prototype. After receiving feedback, we once again made changes to the prototype and met with our third participant.

Our third participant was a 19 year old computer science major at SIUE. He went through the tasks on the latest iteration of the prototype while providing feedback. After his responses, we gathered our results to make the final paper prototype.

During the testing process, we learned how to effectively conduct tests, and got better at this after working with each participant. In particular, we found that people have pre-existing ideas of how software should work, and our product should align with those features to be usable. We also found that participants did best during usability testing when they had a clear goal to achieve or task to complete. But, at the end of the test, it was also helpful for the user to just wander around the UI, so we could see how a user might learn or navigate the program in their first interaction. Any time the user got confused, we made sure to ask what was confusing and we would get a better idea of how to narrow down the design.

Overall, the testing process was incredibly helpful in refining our design. The results that we found will be discussed in the next section.

Testing Results

Heuristic Evaluation Results:

Across the two heuristic evaluations of our project, we found several things we were able to improve upon.

In the first evaluation, though it was noted that the overall design of the interface was efficient and minimal, we were told that the placement of our “learn more” tab was too high, and that it should be moved lower (effectively given a lower priority) than other tabs that offer the user more information on settings or use of the software. This violation - the learn more tab having a higher priority than more use-informative tabs - was labeled as a violation of the “user control and freedom” heuristic, though it might have also fit under the “flexibility and efficiency of use” heuristic as well.

In the second evaluation, we noted violations of both the “user control and freedom” heuristic as well as a violation of the “flexibility and efficiency of use. The violation of “user control and freedom” was fixed by adding a checkbox popup saying “don’t show me again” that allowed the user to quickly and easily disable popup warnings for a particular site or contact. The violation of “flexibility and efficiency of use” was addressed by adding a link in the “history” tab that redirects the user to the relevant section in the “learn more” tab, allowing the user to very easily find relevant information on scams they’ve (potentially) already encountered.

In all, though there weren’t too many noted heuristic violations, the ones that were uncovered in this step were pretty major, and the changes we made to address them make quite a difference in the overall look and feel of the final project.

Usability Test Results:

Test 1

The first task was used to record his interaction with an email scam using our app. After receiving a suspicious email, and getting notified by our program, the user went to learn more information about the scam. From there, he viewed the description of the scam that he encountered. After this he looked through the settings and options that the app had in preventing and notifying the user about scams. He noted that the "learn more" indicator could be made clearer, and we should change the settings menu to have more obvious options to enable/disable parts of the program. This led us to add a more clear button on the *History* tab that indicates that it takes you to learn more information about the scam.

In our second task, we observed the user interact with a social media account setup that was asking for too much information. When the user was prompted to enter a social security number, the program interrupted the user to indicate a scam. Out of interest, the user disabled this popup. This resulted in the event being recorded, but not blocked by the program. The user suggested that our program notify the user of similar sites that are not scams. This led us to create the *recommended sites* dropdown menu for any suspicious links like "FaceSpace.com". He also suggested that the popup be prompted earlier, as soon as the threat is recognized. We simply just brought up the popup before the user entered any information to begin with. After the two tasks were completed, we asked the participant for questions. He asked how the program is able to detect scams, and if it is invasive to the user's privacy. He also asked if the program would be resource-heavy. These are both things that we now indicate to the user with the inclusion of a warning saying that we do not save the user's personal information and a more detailed interface of the *Popup Blocker* tab.

Test 2

We started the test with the first task and the first thing he did was press the newly implemented "Stop receiving warnings from this site/contact" checkbox. This was an unintended issue that we came across and asked him why he pressed it. He said that on instinct he pressed it because that is what he normally does with those popup messages. He then suggested that we should not make it a checkbox and just a link to the pop-up blocker settings. We added a different type of button which redirects the user to a confirmation.

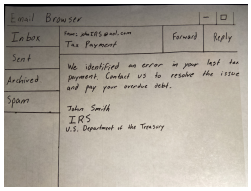
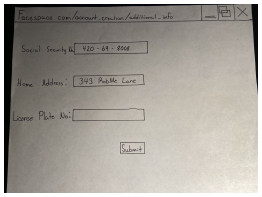
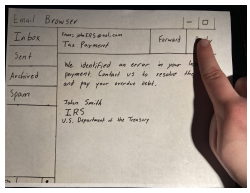
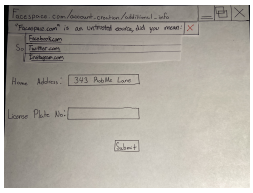
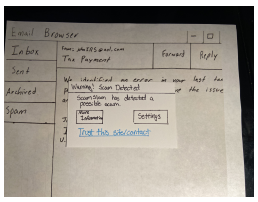
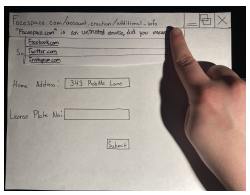
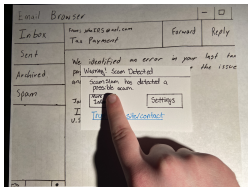
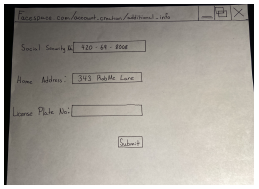
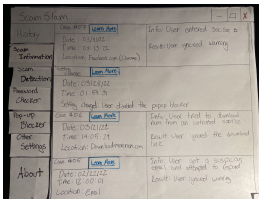
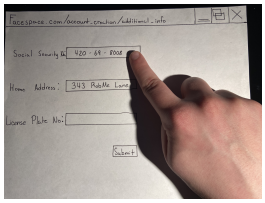
After we finished with the first task, we moved onto the second task. We told him to act as if the link was there and that made him click the other options. He pressed the "settings" button which took him to the pop-up blocker settings where he then looked through the settings given. He then asked to go back to try out the "learn more" button which directed him to the history tab. Then we ran into another problem with the revisions to the prototype, since he couldn't tell for sure if the newly added "learn more" button on each of the scams was a button or just a label, since they looked so similar to each other. We added a new color to the button which differentiated it from the previous prototype.

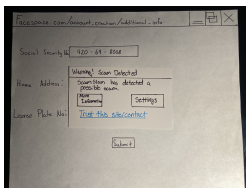
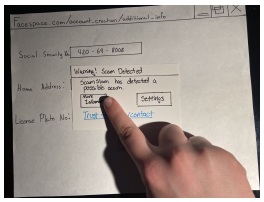
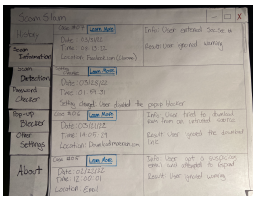
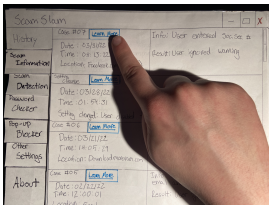
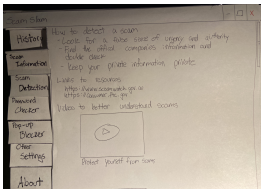
Test 3

The first task was presented to him and he pressed the “learn more” button, but had a few things to say about it before. He recommended that we change the popup even further than the second revision we made. Using this recommendation, we got rid of the minimize and the exit button entirely and changed the popup blocker shortcut to a trust site or contact button. In addition to those changes, we plan on having a confirmation popup to make it more difficult to ignore our warnings. The participant then continued onto our user interface and thought that it was well made.

We continued with the second task and the participant noticed our first revision and thought it was helpful. He stated that he would have used this as an option, but he was curious about the other parts of the prototype. The popup appeared as soon as he went to enter the private information and selected the “settings” button. The participant thought that the theme option was a nice touch and had no notable issues with the most recent revision.

Final Paper Prototype: *Complete paper prototype shown in Appendix Figure 2*

Task 1: Determining if a message is suspicious		**Task 2: Keeping private information private**	
	The user is sent a suspicious message from an untrusted source. Our software does not read the email or contact if the user does not interact with it.		The user is trying to create a social media account from a website called “Facespace”.
	The user replies to the email, unaware that the message is a fraud.		Our software detects that the page is a scam and suggests different options that are similar, but from trusted sources.
	Our software then goes through the contact and email to check for red flags, which are found because the email address is falsely claiming they are the IRS.		The user ignores the message because they are confident that the site is credible.
	The user is curious and wants to know how it was flagged as a scam.		Since the recommendations were ignored, the user is taken back to the original webpage.
	The user is taken to the “History” page which shows why, when, and the location of the scam that was detected.		The user then starts entering private information that should not be shared.

	Our software scans the site that is untrusted and detects that it is an untrusted source that is asking for a social security number.
	The user takes this warning more seriously and is attempting to find out why the software warned them.
	The action the user took in the popup redirects them to the “History” tab.
	The user wants to find out why the scam was detected, so they click on the “Learn More” option.
	The user is taken to the “Scam Information” tab which details that “Facespace.com” is an untrusted source that asked for information that was not necessary when making a social media account.

Pop-up Warnings and Notifications *Figure 2A*

Warning about a potential scam being detected. Updated so it is much more difficult to just click off by accident and makes the user actively pay attention to the warnings given. The confirmation pop-up was added with the second revision, made to make the user rethink ignoring the warnings our system produced. This notification is an addition with the third revision, made to inform the user that the information from a scam is recorded in our software, even if the popup was ignored or blocked.

Recommendation Search Bar *Figure 2B*

This is an addition that was made during the first revision. The recommendations help stop a potential scam before it can even start.

Suspicious Website and Email *Figure 2C*

FaceSpace is a fake social media website that was made to scam information from users. An email browser with a suspicious email asking for money.

History Tab *Figure 2D*

The "History" tab is the first page of the UI and the page where the user is directed to whenever they press the "learn more" button on the pop-up or the "History" link on the notification. There was an addition of a "Learn More" button on each scam that was made in the first revision and made more clear in the second.

Scam Information Tab *Figure 2E*

The "Scam Information" tab is the second tab of the UI which helps the user learn about both scams in general and information about a specific scam that was recorded in the "History" tab. The name of the tab was switched from "Learn ways to protect yourself" to "Scam Information" in the first revision, since it was more concise.

Scam Detection Tab *Figure 2F*

The "Scam Detection" tab is the third tab in the UI and the first tab with settings. The user can uncheck any of the types of scams they would not like a pop-up to appear for. Each of the boxes are checked when the software is first installed. The first revision had the list changed from circles to boxes to indicate that more than one is selectable, and the option of online forms was included.

Password Checker Tab *Figure 2G*

The "Password Checker" tab is the fourth in the UI, but the second in settings. This helps users keep their passwords safe and lets them test passwords to see how safe they are. A few additions were made to make the wording more clear to users and we included a disclaimer that states we don't save passwords and other private information.

Pop-up Blocker Checker Tab *Figure 2H*

The "Pop-up Blocker" tab is the fifth page on the UI, but the third in the settings. This makes the user have more control over what and who the pop-up appears for. The only addition to this tab was the inclusion of disabling contacts that was made during the first revision.

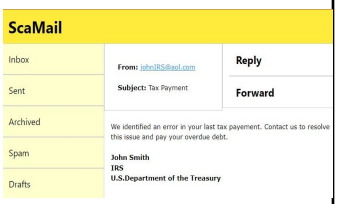
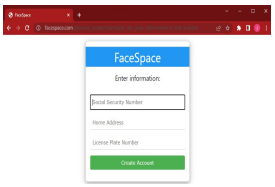
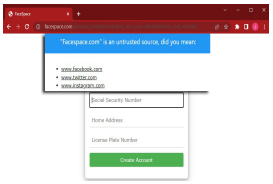
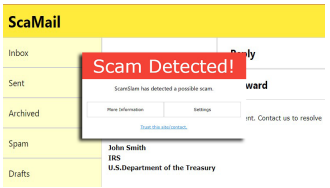
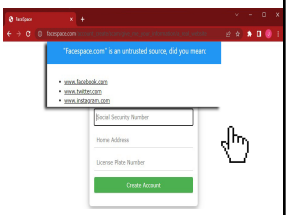
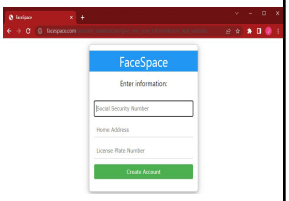
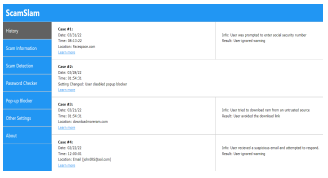
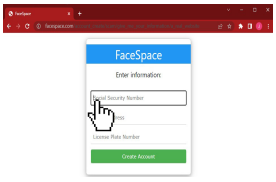
Other Settings Tab *Figure 2I*

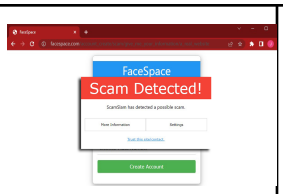
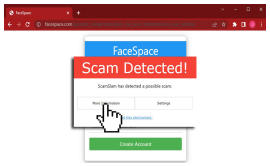
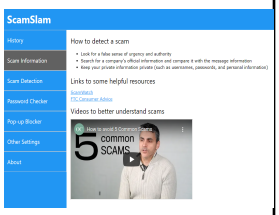
The “Other Settings” tab is the sixth page in the UI and the last page of settings. This covers more general settings and there were no additions to this page on any of the revisions.

About Tab *Figure 2J*

The “About” tab is the last page of the UI. This is general information about the software and our group that had no additions throughout the revisions.

Digital Mockup: *Complete digital mockup shown in Appendix Figure 3*

Task 1: Determining if a message is suspicious		**Task 2: Keeping private information private**	
	The user is sent a suspicious message from an untrusted source. Our software does not read the email or contact if the user does not interact with it.		The user is trying to create a social media account from a website called "Facespace".
	The user replies to the email, unaware that the message is a fraud.		Our software detects that the page is a scam and suggests different options that are similar, but from trusted sources.
	Our software then goes through the contact and email to check for red flags, which are found because the email address is falsely claiming they are the IRS.		The user ignores the message by clicking elsewhere on the page because they are confident that the site is credible.
	The user is curious and wants to know how it was flagged as a scam.		Since the recommendations were ignored, the user is taken back to the original webpage.
	The user is taken to the "History" page which shows why, when, and the location of the scam that was detected.		The user then starts entering private information that should not be shared.

	Our software scans the site that is untrusted and detects that it is an untrusted source that is asking for a social security number.
	The user takes this warning more seriously and is attempting to find out why the software warned them.
	The action the user took in the popup redirects them to the “History” tab.
	The user wants to find out why the scam was detected, so they click on the “Learn More” option.
	The user is taken to the “Scam Information” tab which details that “Facespace.com” is an untrusted source that asked for information that was not necessary when making a social media account.

Pop-up Warnings and Notifications *Figure 3A*

Warning about a potential scam being detected. This popup remained the same from the paper prototype except for minor formatting changes to make it look more urgent. A confirmation when the user presses the "trust this site/contact" link. This went through the same changes that were made in the popup itself. A notification that pops up in the corner of the user's screen to inform the user that the data was saved and lets them open the "History" tab. This notification had the same changes that the other popups had.

Recommendation Search Bar *Figure 3B*

The "Recommendation Search Bar" is a popup that appears under the URL of any untrusted sites and gives trusted options to the user. This remained the same from our paper prototype with minor formatting changes.

Suspicious Website and Email *Figure 3C*

A fake social media website that was made to scam information from users. Minor formatting changes were made from the paper prototype. An email browser with a suspicious email asking for money. Minor formatting changes were made from the paper prototype.

History Tab *Figure 3D*

The "History" tab is the first page of the UI and the page where the user is directed to whenever they press the "learn more" button on the pop-up or the "History" link on the notification. The digital mockup changed the spot of the "Learn More" link to the bottom of the scam data.

Scam Information Tab *Figure 3E*

The "Scam Information" tab is the second tab of the UI which helps the user learn about both scams in general and information about a specific scam that was recorded in the "History" tab. This tab remained similar to our paper prototype in content but was cleaned up a bit with formatting.

Scam Detection Tab *Figure 3F*

The "Scam Detection" tab is the third tab in the UI and the first tab with settings. The user can uncheck any of the types of scams they would not like a pop-up to appear for. There were a few changes made to this tab which help give the user more control over when they would like the pop-up to appear. There was also a bit of text added to make the user better understand what the settings mean.

Password Checker Tab *Figure 3G*

The "Password Checker" tab is the fourth in the UI, but the second in settings. This helps users keep their passwords safe and lets them test passwords to see how safe they are. A few changes were made to make the digital mockup look better. The most important addition was to tell the user how long a password would take to crack by a bot.

Pop-up Blocker Checker Tab *Figure 3H*

The “Pop-up Blocker” tab is the fifth page on the UI, but the third in the settings. This makes the user have more control over what and who the pop-up appears for. This tab was cleaned up a bit from the paper prototype and we decided to add a few trusted sources to show how the user can tell which sites and contacts are trusted.

Other Settings Tab *Figure 3I*

The “Other Settings” tab is the sixth page in the UI and the last page of settings. There were only minor formatting changes made from the transition to a digital mockup, like having the theme buttons more intuitive to the user.

About Tab *Figure 3J*

The “About” tab is the last page of the UI. This tab experienced the most changes from any of the other tabs. We included a history of each prototype made and included a FAQ, which helps users with many of the problems they may experience with the software.

Discussion

What We Wanted To Do

The original problem space we decided to work in was that of scams - though at first we had no specific vision of how we intended to do this, we wanted to find a way to somehow protect individuals vulnerable to scams and deception aimed at their finances or personal information. At first, our target community was the elderly, a demographic notoriously vulnerable to this kind of malicious scheming, but in the end we decided that the target for our project would not only be those that are vulnerable, but anyone conscientious about the safety of their information and finances.

What We Did

Our first sketches were quite varied in design and separate in focus. The included: a desktop application that could recognize and redirect suspected "scam" emails, a phone or computer application that could read a program prior to being downloaded and alert the user to any suspicious functionality, a phone app that could block calls or messages from seemingly suspicious numbers, an app that would be able to read and succinctly summarize TOS's when a user downloads a program or signs up for a service, and an application that recognizes if a popup seemed to have malicious intent or not.

In the end, we decided that none of these ideas were solid enough to stand up on their own, and that a combination of their functionality might be something more substantial. Though we learned a lot throughout our testing and iterative design, our final product was exactly that - a software suite (theoretically for both mobile and desktop) offering a varied and wide list of anti-scam functionality, including all of the features from our initial sketches and more.

What We Learned - Problem Space

Pertaining to the problem space of scams, we learned many things, the most important being that the number one protection against them is education and alertness. At the end of the day, anyone can ignore a warning that something might potentially be a scam, so both the first and final lines of defense are one's own knowledge and intuition on each potentially suspect situation.

What We Learned - Design

In the way of design, our group learned that you shouldn't become attached to any particular initial design choices. Throughout the process of research and testing, many changes were made to our project, and though the core idea was still there in the end, the final product looked far different than it did in its initial state. Much of what we thought was "core" to the design of the project was changed, sometimes quite majorly, throughout our iterative design process. In a sense, none of our initial choices were safe, and almost any design elements were subject to change as we gathered more information and refined our process.

Appendix

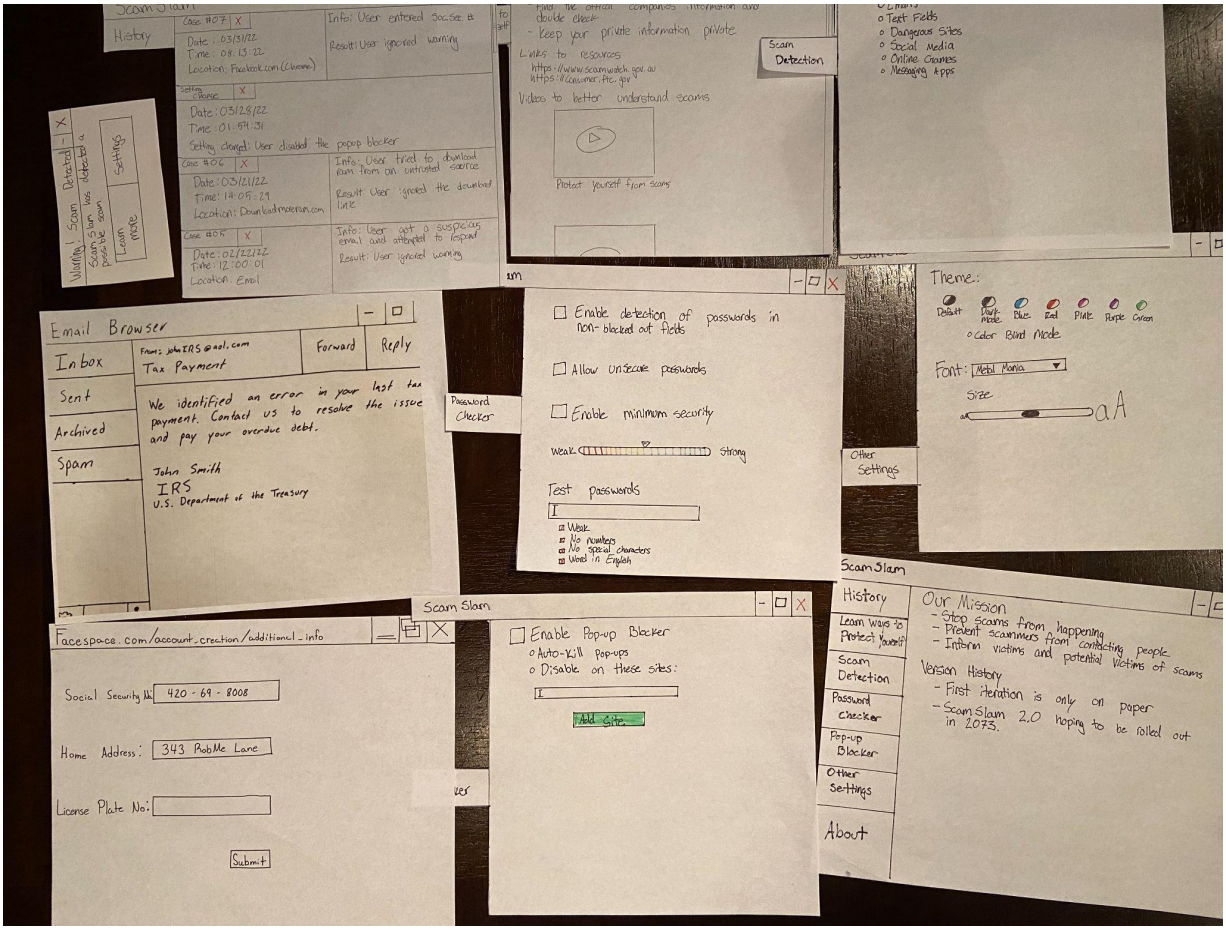


Figure 1: Complete initial paper prototype

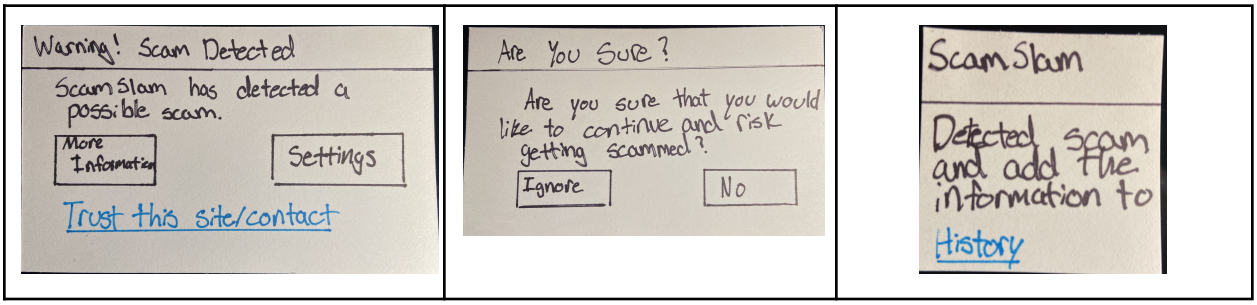


Figure 2A: Pop-Ups and Notifications

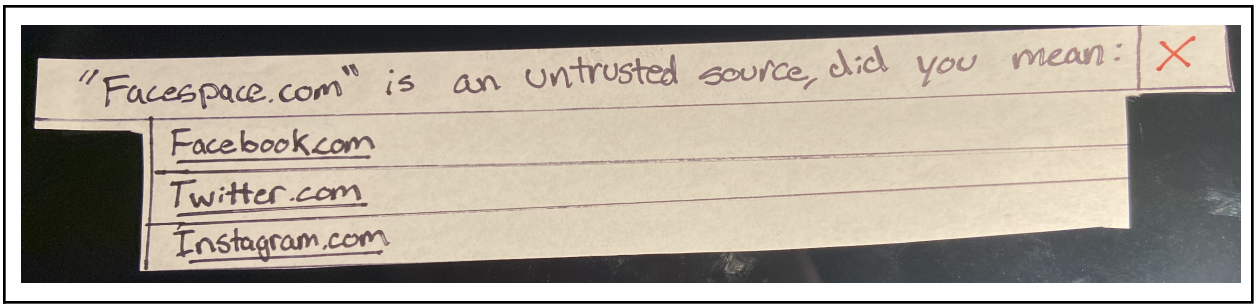


Figure 2B: Recommendation Search Bar

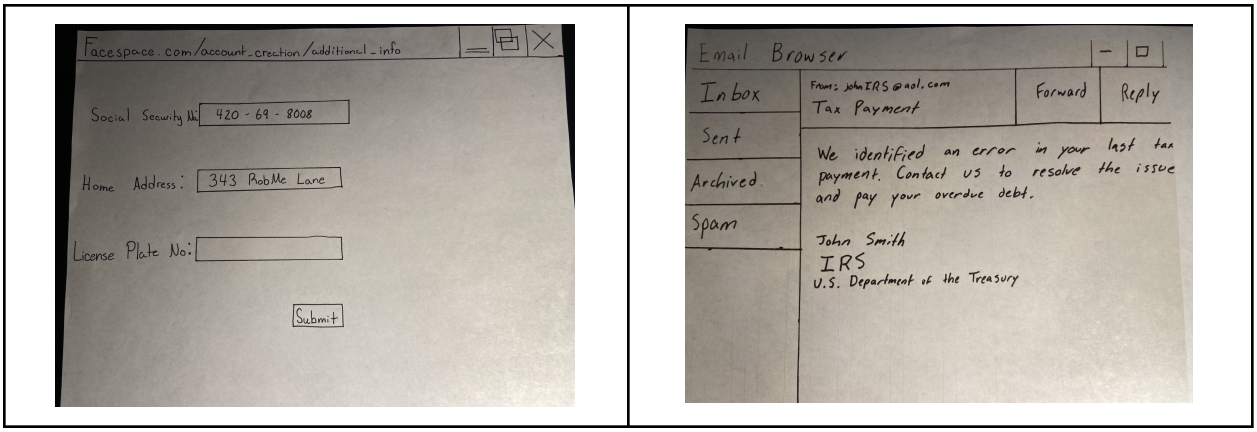


Figure 2C: Suspicious Website and Email

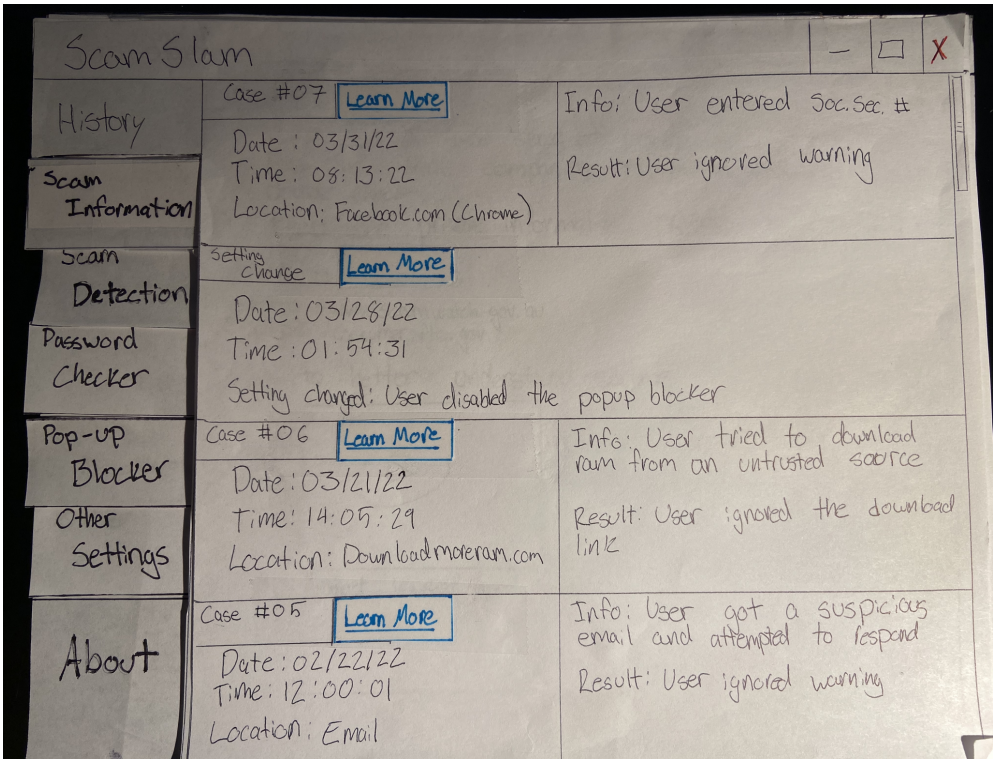


Figure 2D: History Tab

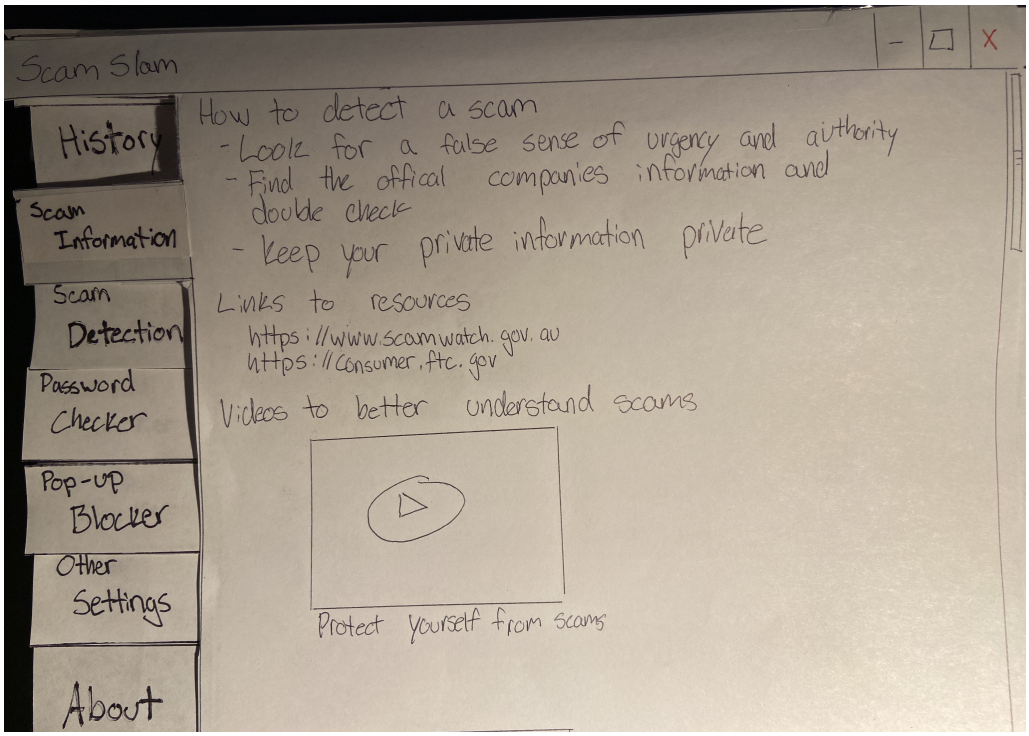


Figure 2E: Scam Information Tab

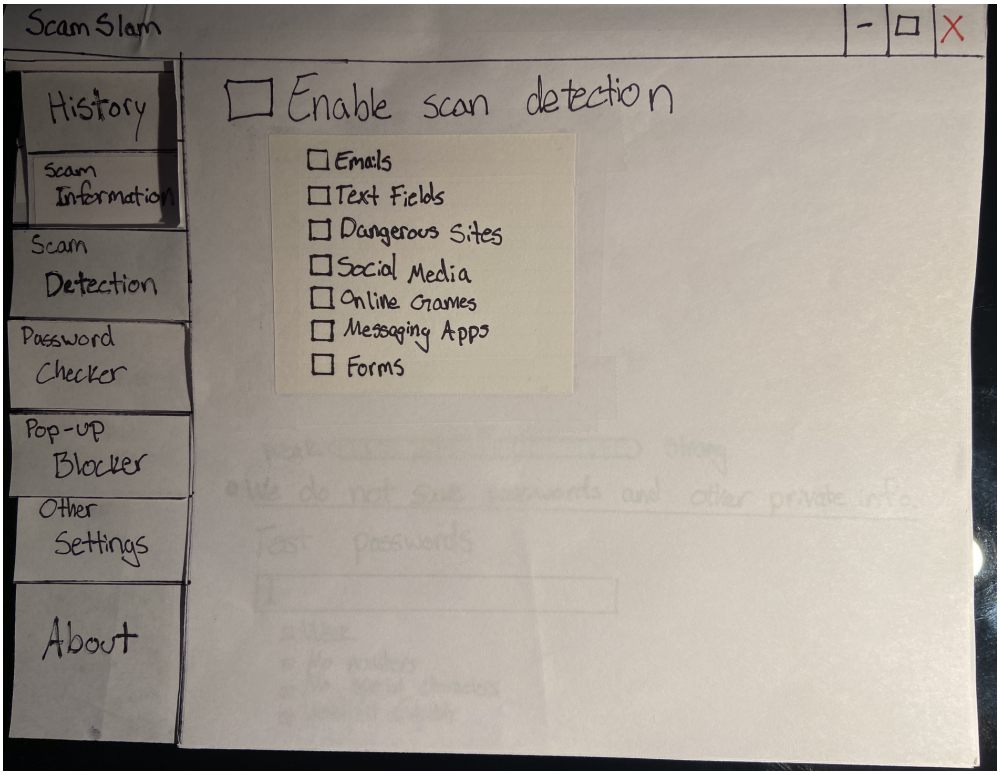


Figure 2F: Scam Detection Tab

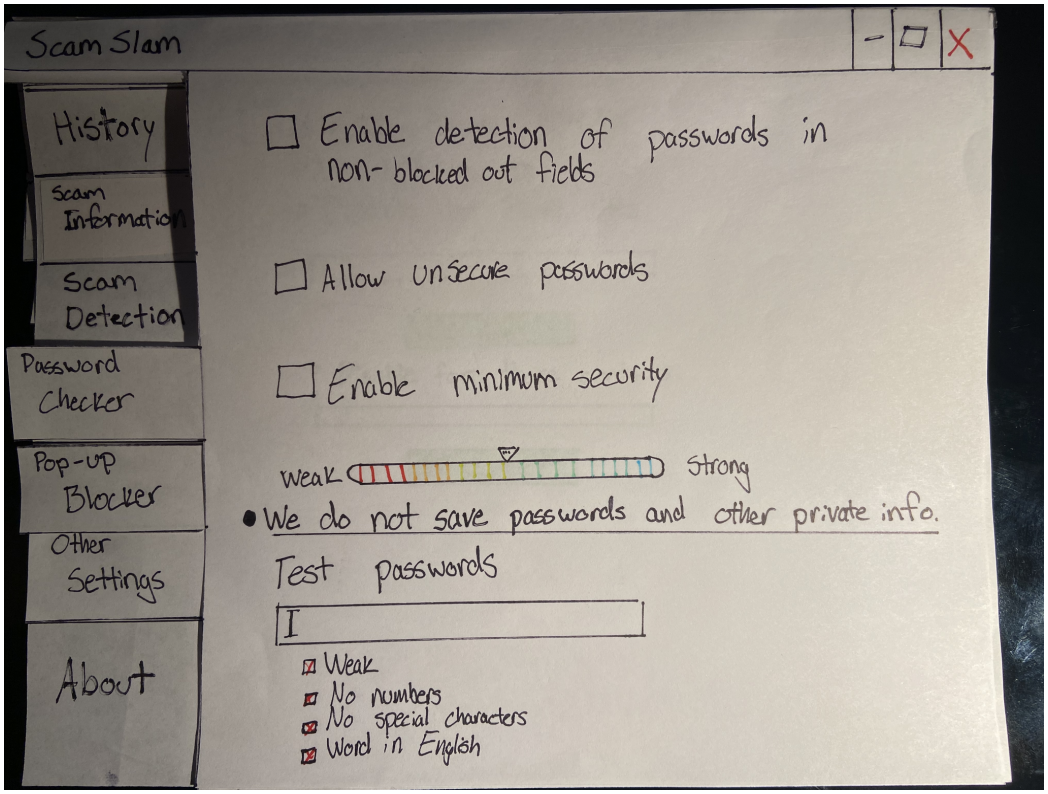


Figure 2G: Password Checker Tab

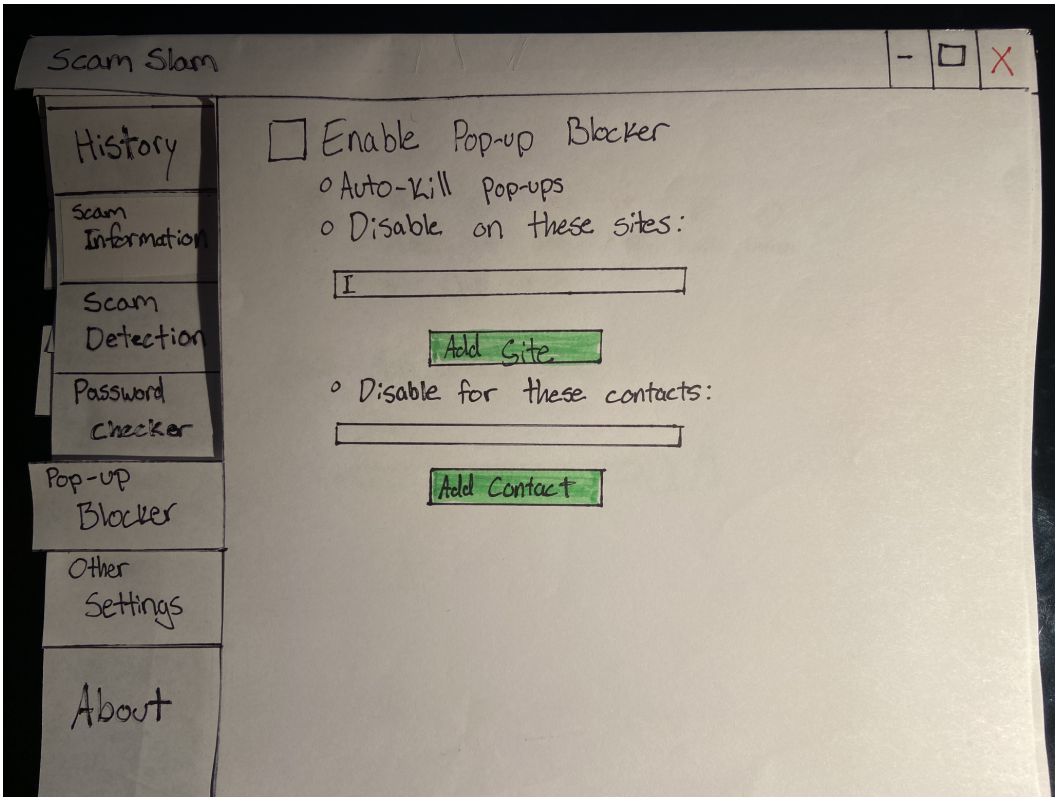


Figure 2H: Pop-Up Blocker Tab

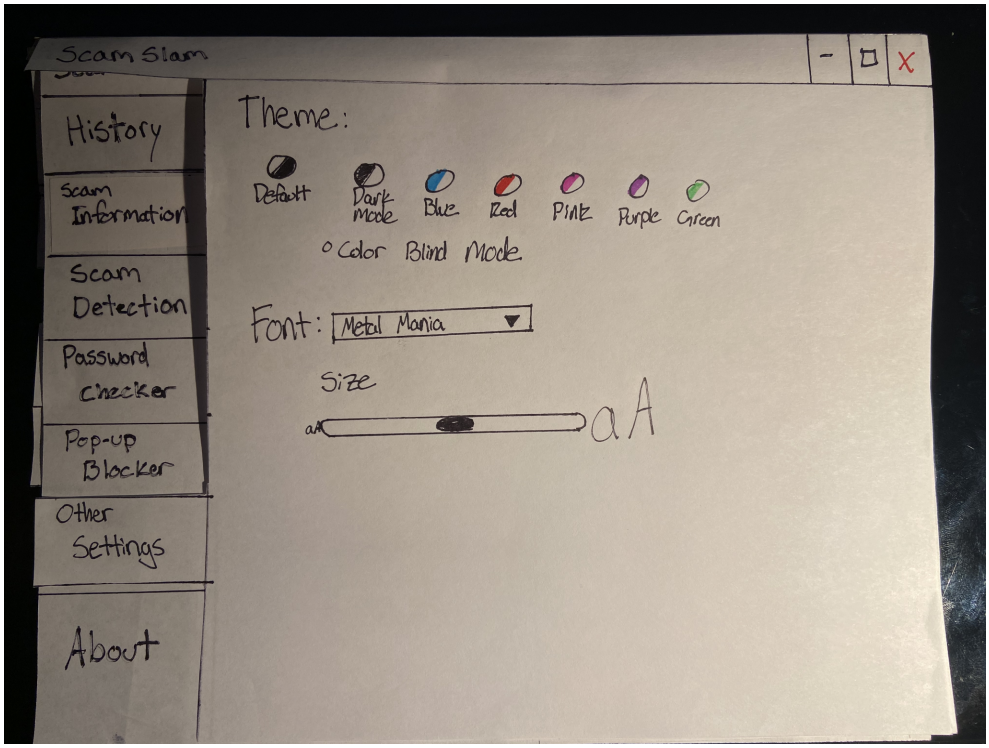


Figure 2I: Other Settings Tab

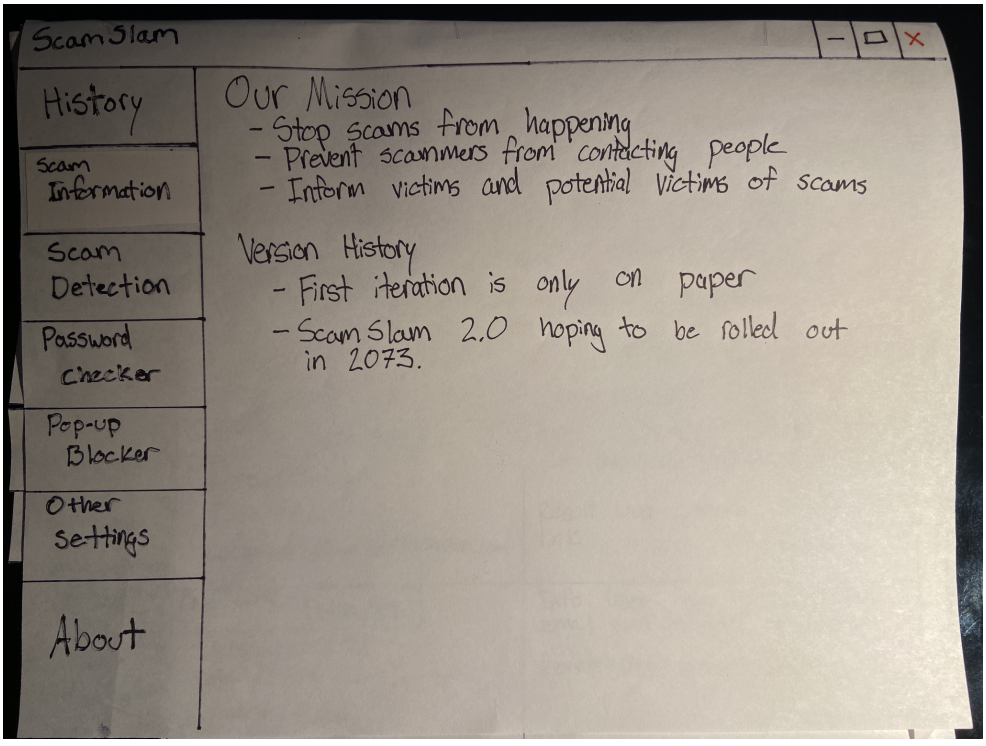


Figure 2J: About Tab

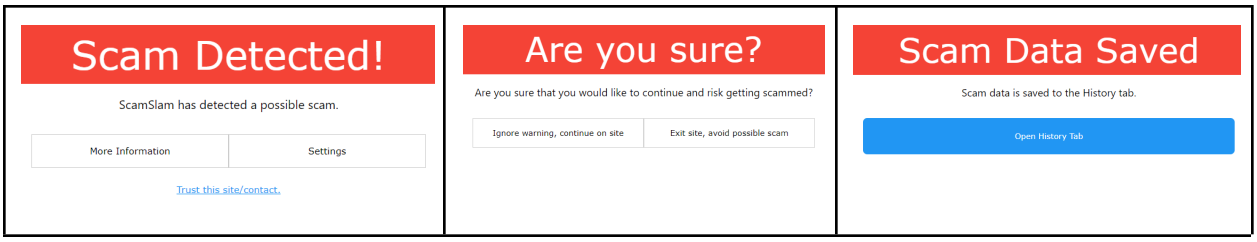


Figure 3A: Pop-Ups and Notifications

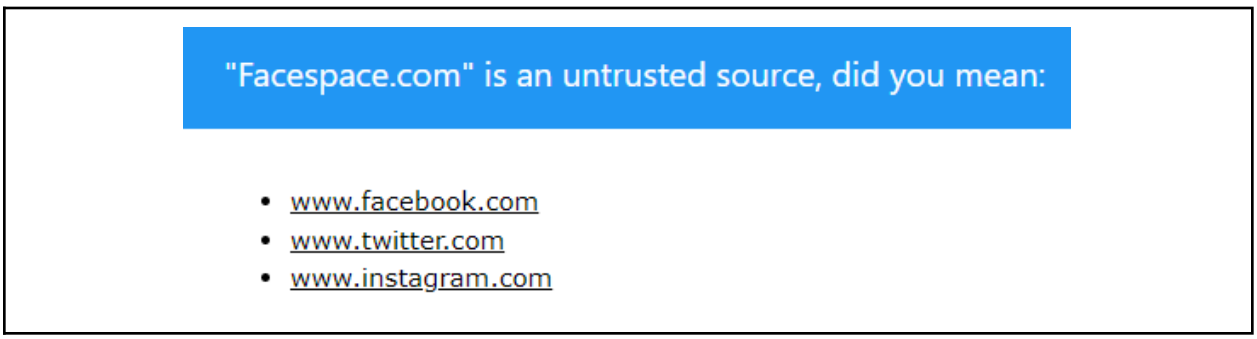


Figure 3B: Recommendation Search Bar

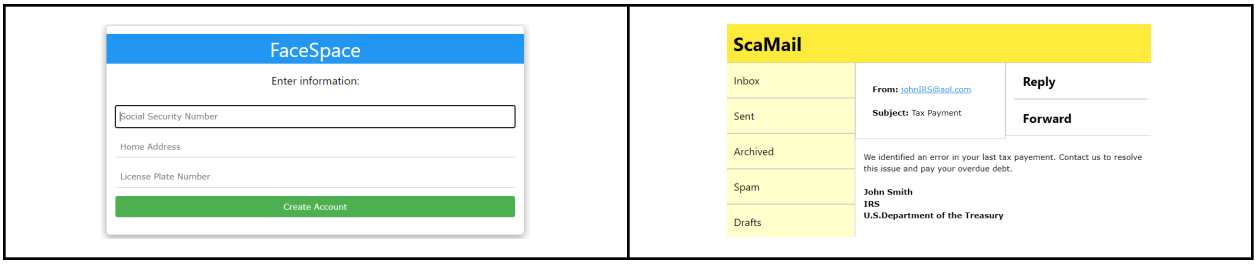


Figure 3C: Suspicious Website and Email

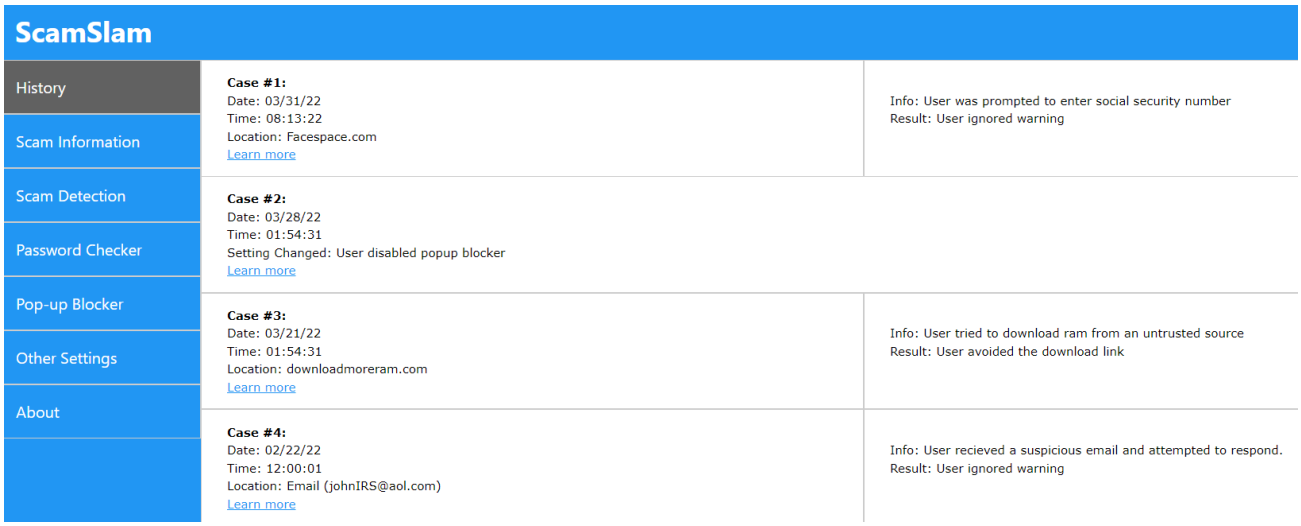


Figure 3D: History Tab

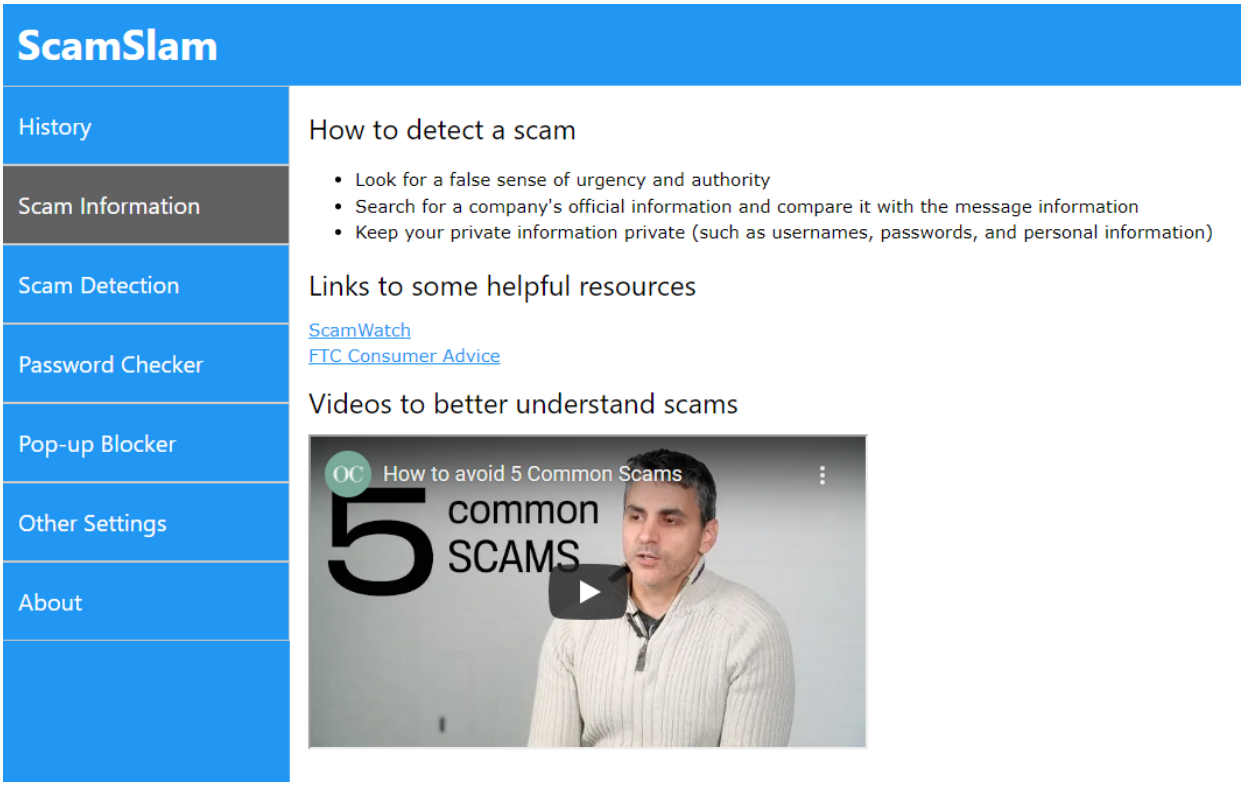


Figure 3E: Scam Information Tab

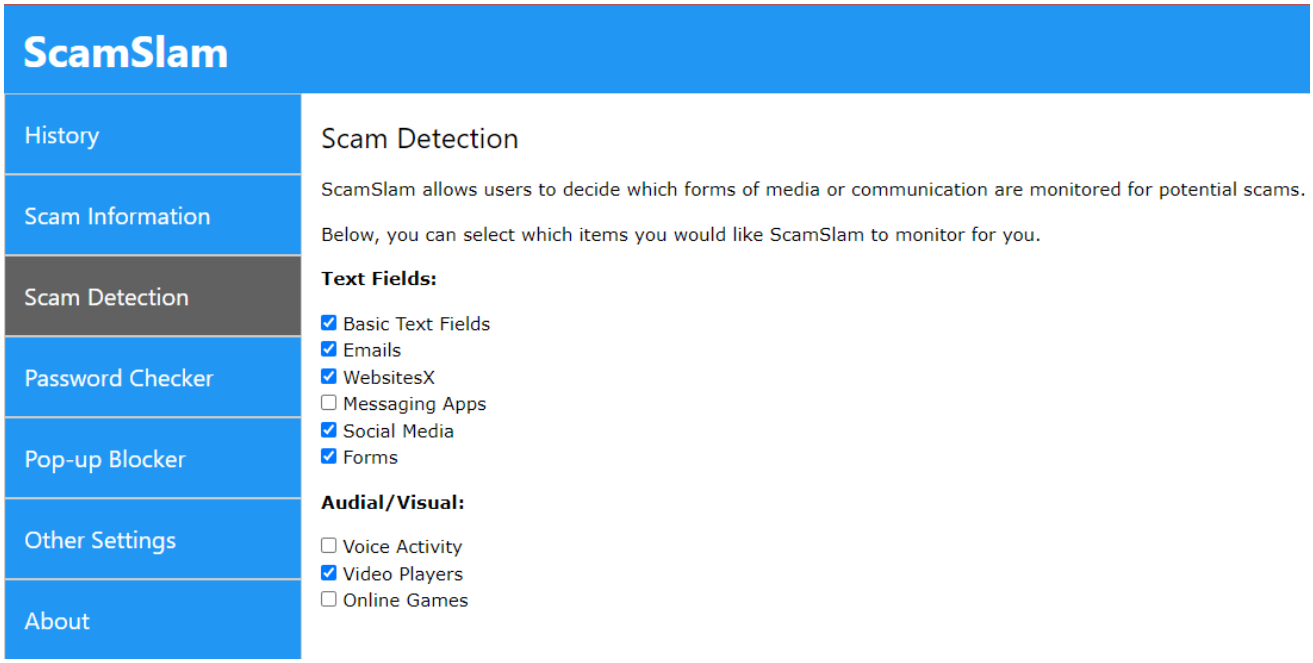


Figure 3F: Scam Detection Tab

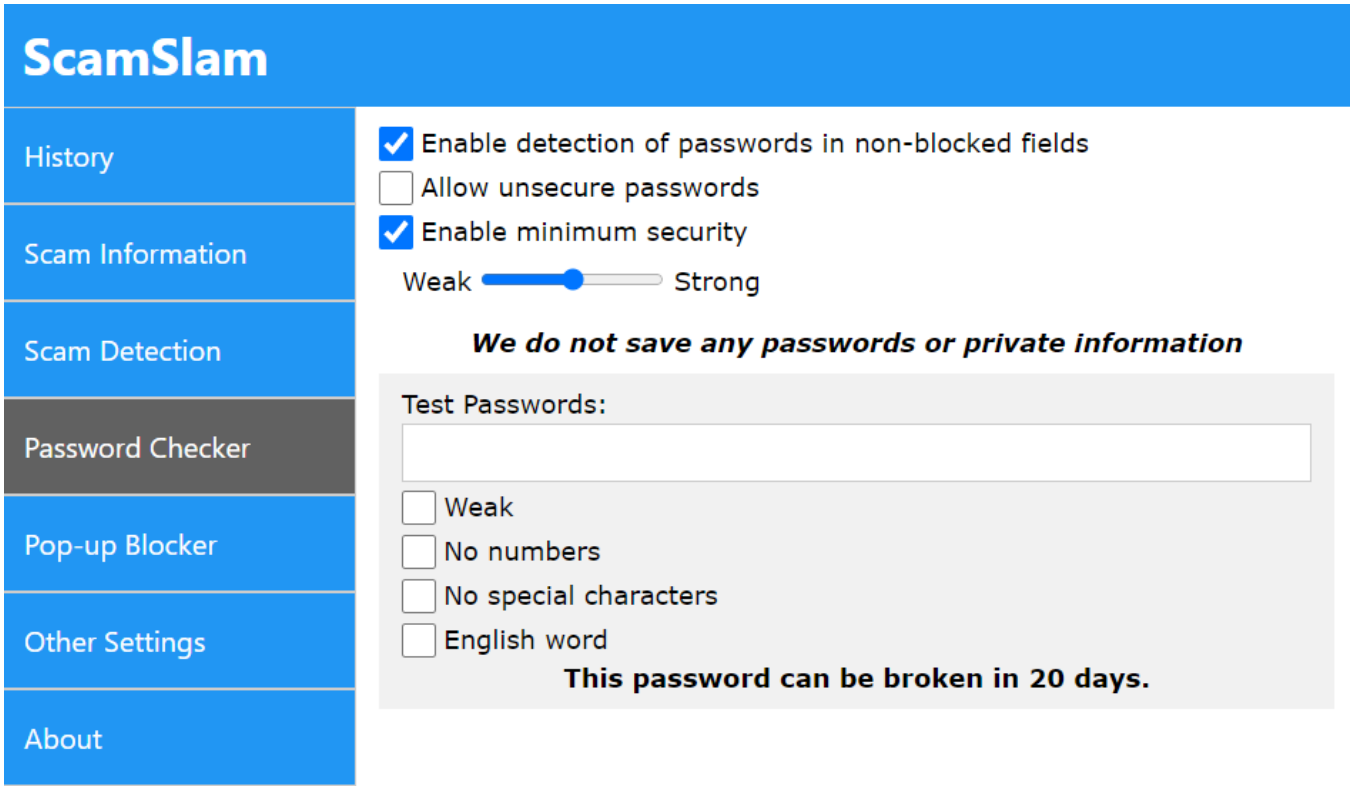


Figure 3G: Password Checker Tab

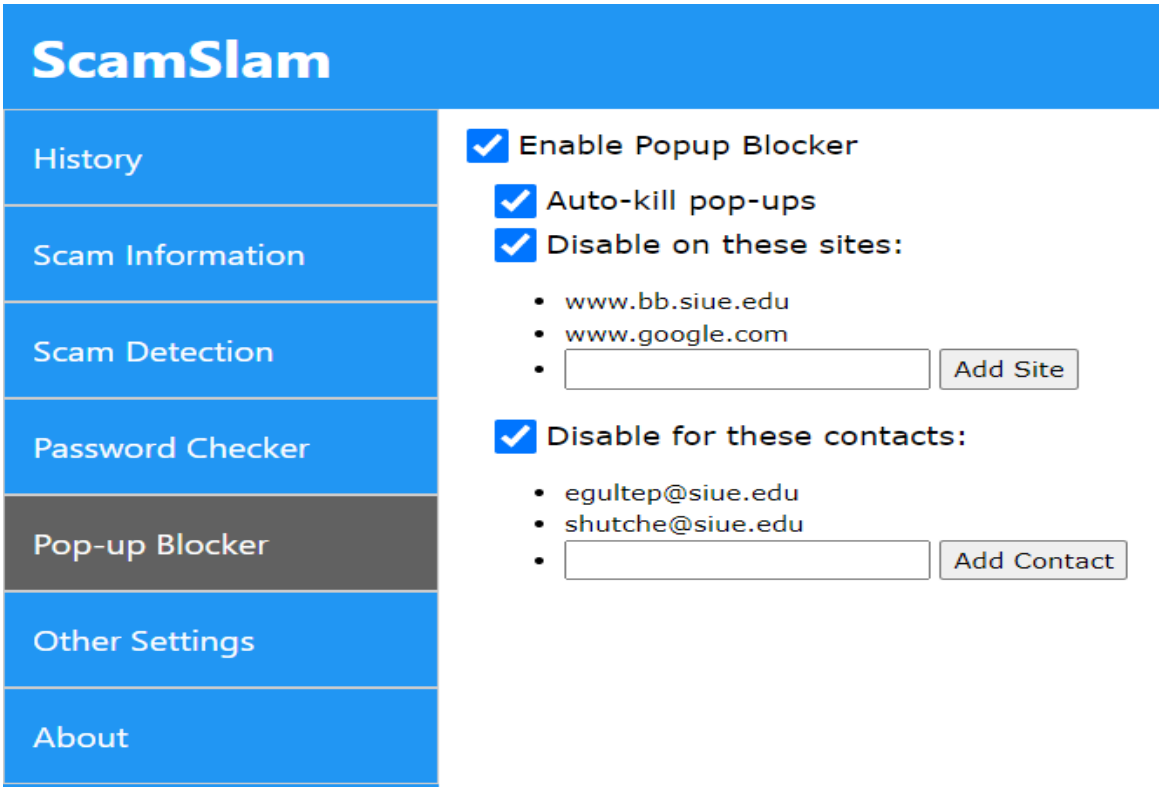


Figure 3H: Pop-Up Blocker Tab

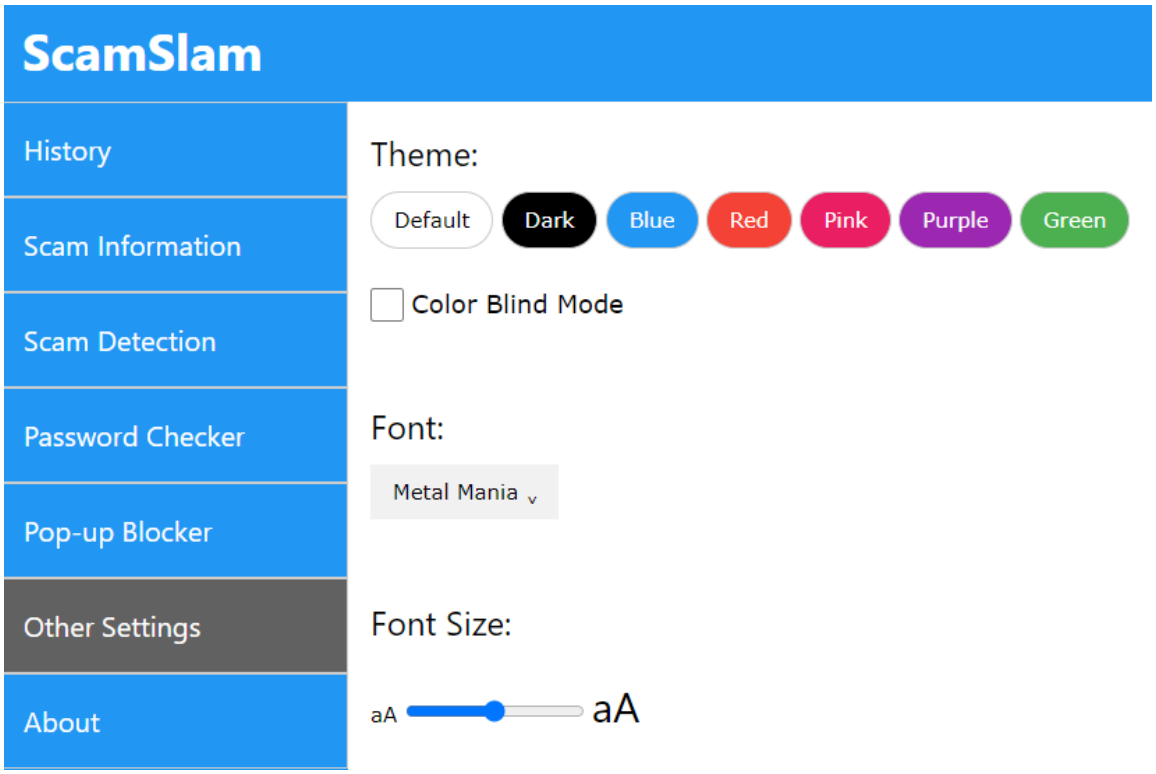


Figure 3I: Other Settings Tab

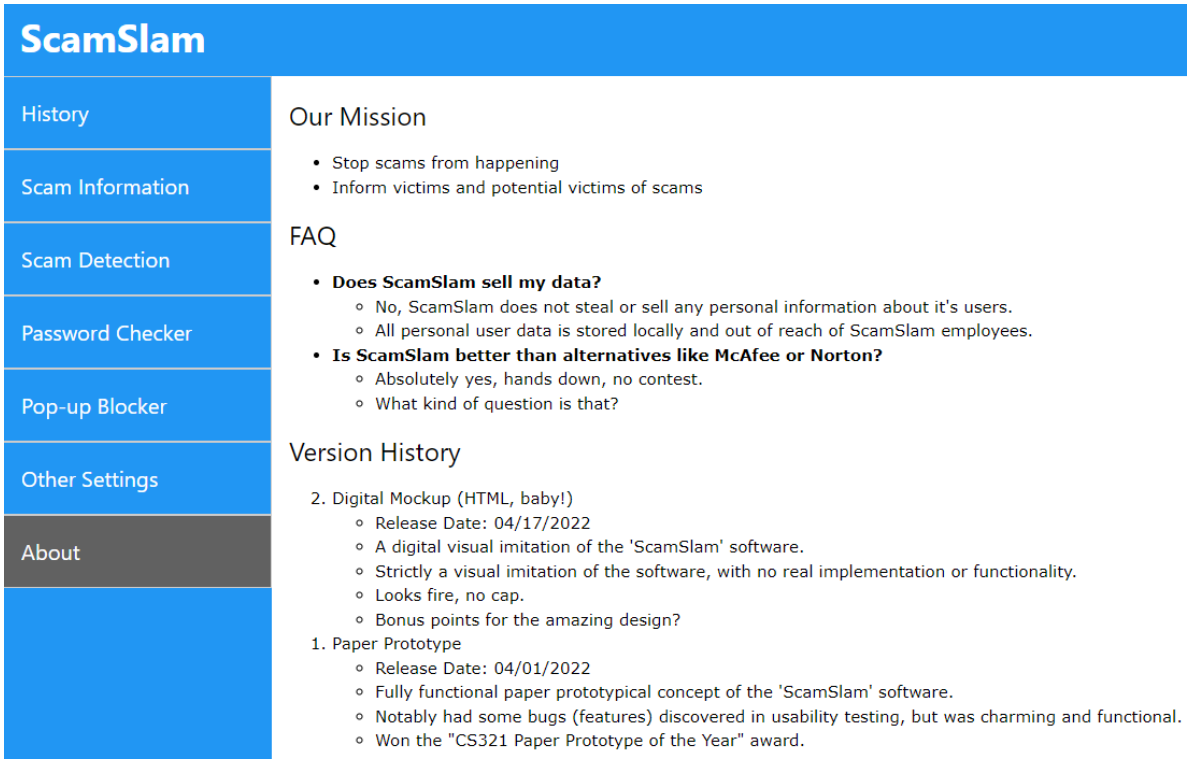


Figure 3J: About Tab