365 Security Guard: An AI-Powered Scam Detection Tool Designed for College Students

Qingyue Yang
Department of Computer Science
University of California, Davis
yqmyang@ucdavis.edu

Lily Hu
Department of Computer Science
University of California, Davis
lihu@ucdavis.edu

Tianren Chen
Department of Computer Science
University of california, Davis
tchchen@ucdavis.edu

Chenghao Wu
Department of Computer Science
University of California, Davis
chgwu@ucdavis.edu

Ryan Liao
Department of Computer Science
University of California, Davis
Ryliao@ucdavis.edu

Yanming Luo
Department of Computer Science
University of california, Davis
yamluo@ucdavis.edu

ABSTRACT

Currently, online scammers employ modern deceptive techniques to deceive university students for job employment through fraudulent promises and tricking methods. Student vulnerabilities while using the internet occur because they lack funds and possess minimal understanding of scams. The solution introduces 365 Security Guard as an AI-based browser extension which protects university students from fake schemes. The tool operates differently from antivirus software and spam filters through AI real-time detection of potential scams that automatically triggers real-time alerts during transactions.

The user experience of our tool reaches maximum effectiveness by implementing Human-Computer Interaction principles to minimize cognitive burden and let users adapt settings for enhanced visibility. All the local detection processes of the tool guarantee user data security because there is no data collection. Through the 365 Security Guard system users can easily utilize its interface because it provides single-click installation features and customized alert settings along with a "Deal Check" tool dedicated to verifying discounts and job opportunities. Our service protects students from scams by offering two functional areas: preventative scam detection as well as expert post-scam recovery assistance to guide them through scam-related challenges. Research studies for user experience and usability support the effectiveness of our solution because it shields students from scams while providing them better control combined with increased awareness.

1 INTRODUCTION

Online fraud stands as the main challenge students encounter in college setting. The combination of youth age with inexperienced handling of money under pressure makes students vulnerable to scams. Lack of experience among young people combined with financial challenges makes them vulnerable to scam attempts.

Based on our interview research revealed that young students between 18 and 24 years old had already experienced online scams. Such as, staff at the senior level received bogus employment documents sent to their email. A convincing design of the email prompted the recipient to disclose personal data. The student discovered the message was fraud after the damage had already been done to his wrong decisions. Students became scam victims after their education institution delivered false phishing correspondence through their emails. The attack trap victims through links that required passwords as input which afterward blocked students from their accounts. The same official appearance of scammers' messages makes them dangerous for students.

Other students shared similar experiences. An academic member gave money to a fraudulent internet group that promised high returns through cryptocurrency investments. The victim sent money to scammers yet the criminals disappeared right afterward. Through social media the student acquired cheap concert tickets and got blocked from the seller right after they paid. A present-day university student spent their money by trying to unlock a SIM card using unauthorized web services.

Students commonly demonstrate their annoyance at being obligated to watch security alerts through present-day security systems. Students ignored security warnings which they found irrelevant despite their frequent appearance because they occurred more than 80 percent of the time. Students have adopted a habit of dismissing genuine security threats after their exposure to excessive security warning messages.

The students who lost their funds through online payments discovered no available way to recover their lost funds. The encryption used by the system prevented any users from retrieving their funds since it provided complete security. They felt helpless and frustrated.

365 Security Guard solves these problems. Users benefit from a user-friendly interface provided by the browser extension made for college students. The system generates important information in minimal warning alerts. Students can adjust the warning frequency through the system to prevent getting sidetracked. The extension offers educational materials featuring details about the leading scams that aim at students which consist of fake job offers plus phishing attempts and online shopping frauds.

Through its service the security guard team helps customers find methods to recover from scams. Students who lose money receive direct instructions through the security guard service from 365 Security Guard. Through the provided guidance students learn how to stay away from helplessness. We developed an efficient tool by precisely evaluating student experiences to produce 365 Security Guard which offers enhanced browsing security and scam protection. This extension satisfies the bona fide requirements of students to deliver innovative enhancements in online security procedures.

2 BACKGROUND & RELATED WORK

The scams targeted at college students have become a major concern among students. Some college students may lose a large amount of money in some situations which may worsen the financial situation of students at the same time they need money to pay their tuition. The loss of money is hard to recover due to multiple reasons including technical limitations and some policy limitations. Existing cybersecurity tools like Guardio and Aura aren’t designed specifically for college students, which means that those tools tend to provide broad protection without the support required for student-specific scams, such as job scams sent to the email using school email addresses (ucdavis.edu for example). Student-specific scam recovery support is also a key point that needs to be taken into account because the recovery of money could reduce the loss of students and the pressure on them. In contrast, compared with competitors, our product directly solves this problem that may not handled by the cybersecurity tools in the current market by incorporating a "Deal Check" feature, which confirms the authenticity of online offers and jobs by both AI-powered analysis and database comparison, and provides feedback accordingly. The competitors may more focus on preventing risky links and have no direct support for recovering from transaction scams. At the same time, 365 Security Guard also provides actions to recover lost funds and secure accounts.

Our solution integrates many concepts from HCI concepts taught in the class and mentioned in the textbook to make the user use the product easier and make the interaction more enjoyable with the college students who are our target users. It minimizes warning messages and pop-up windows, which can reduce the pressure of the users and ease the process of dealing with online scams. The 365 Security Guard only shows some scam warnings that are clear to see and really important that need to be noticed, instead of making the user remember difficult handling information which indicates the concept recognition rather than recall. On the other hand, the students can customize the alerts according to their needs and interests, which means that they get only the alerts that they need and avoid getting too much information that they already known. Our solution fills the gap with existing tools and offers a less overwhelming and more user-friendly security experience for college students.

3 DESIGN METHOD

In our design process, we followed the stages of design thinking, Empathize, Define, Ideate, and finally Prototype & Test. During the very beginning of the design process, we decided to start the user research process including interviews and surveys to explore the needs of users after we were assigned the topic cybersecurity. During and after the user research, with the needs of the users getting clearer, we started building a persona of the application and finding out the key pain points via multicycle brainstorming. After all the data from the survey and interviews were collected, we had multiple meetings with the team and sat together on how to improve the experience of the users and how to attract them to use our application. A bunch of new ideas for the design of the application were raised in this stage and a few of them stood out after the discussion with the team and also some discussion with the target users that we interviewed. We kept asking the interviewees for the ideas that we came out with in the group discussion to make sure they could meet their needs. Also, the features and usability of other competitors were the points we cared about, which led us to do a lot of research on that and keep

trying those applications in person. Finally, Money Transfer Intermediary, AI Cybersecurity Education, and Strong Technical Support were considered as the key features of our application to solve the needs of the users and stand out from competitors.

Following the ideas we came up with from brainstorming, we decided to make the 365 Security Guard simple and customizable. We started working with the low-fi prototype that could provide a clear draft of what we were going to do in the high-fi prototype with paper and pen at the same time that the brainstorming began, and kept updating with the ideas iterated. After the brainstorming process and the low-fi prototyping process, we got a structure of the application and almost a clear mind on how to design our final product. With the work we had done in the previous steps, we started working on the high-fi prototype that could better show our products and ideas using Figma. All the team worked together on the prototype and iterated versions until we finalized.

4 UNDERSTANDING THE USERS

To create a scam detection tool that effectively serves college students, our group interviewed eight students from different backgrounds. With the main goal of figuring out how students navigate the internet, their levels of experiences with online scams, and their awareness of cyber security. In addition to that, we also asked our interviewees about how they interact with informative applications on their daily basis, with the hope to get useful information for design and prototyping. Through the user research process, we aim to identify patterns of behavior and the key pain points lead to scams. Our results highlighted the victims' major vulnerabilities, and some important expectations from students that they think would ease the situation.

More than eighty-percent of our interviewees claimed that they are overwhelmed by alerts and warnings. This leads them to ignore both real and false alarms. Many respondents described to us that constant pop-up notifications and browser warnings are disruptive, they would more likely to dismiss them without reading. This common behavior of impatience, ignorance, or assumption is one major factor that contributes to high vulnerability of college students to scams. Our group recalled from the Human-Computer Interaction guides from class, this issue aligns with the principle of recognition over recall, we need to create warnings that are clear, concise, and meaningful. Our goal is to solve the overwhelming users experience that many people currently face and struggle with.

Another alarming result from our interview was that one hundred percent of our student interviewees failed to reclaim their money. And even across the internet, our research is showing that less than twenty-percent of victims have the opportunity to reclaim their funds. One of our interviewees provided an example that demonstrated the difficulty to trace lost funds. They unknowingly leaked their Visa card details and personal information, and had never noticed until several weeks after, where they finally tracked down the unusual activities on their account. Despite contacting their bank actively through phone calls and chat assistance, they struggled to dispute the charge and were unable to retrieve their money. Realization of the scam is important, but recovery is what really can help our users and protect their valuables. That's why 365 Cybersecurity wants to take an extra step in scam detection, by providing immediate prevention steps, such as dispute unauthorized charges, and flag scam websites. We aim to empower victimized students to take action as fast as they could instead of feeling helpless after being scammed.

Learning from advice of our peers, our team makes customization an essential feature in our extension tool. Students have varying preferences on how the tools break down their browsing activities, and why a website was flagged. Some users would expect detail and insightful info, while some peers expect simple notifications. The settings should be flexible between different sites too, with online marketplaces and resale websites, our tool could suggest a customized set of warnings for websites prone to scams. We aim to demonstrate flexibility to our users by ensuring that settings can be adjusted to suit different browsing habits. Our extension will feature customizable notifications for individual preferences, ensuring that our security service would not become an obstacle to their online experience.

5 CONCEPTUAL MODEL OF OUR DESIGN

The 365 Security Guard operates as an AI-based platform that provides students in colleges protection against internet fraud schemes. Through artificial intelligence our tool scans online communication for evidence of scams including phony prices combined with deceptive links and job opportunities that turn out to be scams. Privacy stands as one of the primary design aspects within our product. User data sent to the internet is not an issue with 365 Security Guard because scam detection occurs entirely on the user's device itself. In this part, we adhere to Nielsen's H1 (Visibility of system status) by ensuring users know the system is actively protecting their privacy, and H2 (Match between system and the real world) by processing all information locally as users would expect.

Our system includes a feature named "Deal Check" that stands out as its main component. The Deal Check button enables you to verify promising online deals

which seem too attractive. The tool processes the offer in seconds to provide an assessment about its potential being a fraudulent scheme. The additional feature provides you with needed clarification about whether to trust a deal or move forward by helping you maintain better online shopping and job search control. In this part, we implement Nielsen's H6 (Recognition rather than recall) by offering an intuitive verification method, and H3 (User control and freedom) by allowing users to decide whether to engage with an offer.

People require distinct things in their daily lives. Robotanical Security Guard features customizable functions as a result of different user needs. Users can select alert frequencies while designing the severity detail in warnings. Users possess different preferences regarding scam detections since some seek extensive explanations but others require minimal warnings. The adaptable tool has increased its usefulness because it accommodates various user preferences regarding internet usage habits. Also, the real-time update system serves as a strong advantage for 365 Security Guard. Security tools available in the market require manual updates which leads to missed reporting of new scams because they lack regular maintenance. Since our tool automatically learns during encounters with novel scam patterns it becomes constantly better at identifying fraud attempts. The tool provides your system with automatic protection updates while scammers modify their methods. In this section, we adhere to Nielsen's H7 (Flexibility and efficiency of use) by offering customizable alert settings and H2 (Match between system and the real world) through real-time, adaptive updates.

6 PROTOTYPING – LOW-FI TO MID-FI

For the prototyping process, our team started with the paper sketches of user interfaces. Based on the result from our user research and HCI principles, we started with some ideas about the location of UIs. For the concern about convenience and the least disturbance, we planed to make our 365 security guard functioning as an extension plug-in. For the low-fi prototype, we drew the basic UIs on the paper. We connected the user need from the user research result from the interview analysis. By starting with the hand-written wireframes, we quickly tested the layout ideas created during the discussion and user research results. The main focus about the prototyping is on the user navigation, scam alerts, and customization setting.

First of all, user navigation is the main direction for our users to use our prototype design. It is the major difference between the user-centred design and function-centred design. For user-centred design, users should be involved in the development and process of a product. If a prototype has perfect functionality but its interfaces may cause user errors due to poor visibility, inconsistency, or complexity. A good user navigation can help users to use the prototype like dealing with everyday objects which can behave and meet user expectations.

We planned to use three main menu buttons on the top, the large "power" button as the start button on the middle place, which is the most obvious place, and two buttons for report and close near the button. After clicking the large "power" button, the scam protection will be activated. Clicking it again, it will stop protection. Assume a new user who has no idea about the prototype and no experience on using such an extension. The first thing he will notice when opening the extension is the large power button on the middle. The power button relates to the power button of computer, cell phone, and all different kinds of electronic devices. It generally means "turn on" and "turn off" in users' cognitive model since it is the logic from the real world. When the user tried to click it, the large green tick will show up. Both the color green and the icon tick show the information that the product turns on. WIth the words under the icon, the user will know that he just turned on the power button of 365 security guard. Maybe he doesn't want to turn it on so he clicks the middle button again, which is also based on the logic from the real world power button. The guard will be turned off, as the user expected. It matches the system with the real world. Good visibility of system status also supports that behavior. Even though this user has no experience on the product, he can still figure on the basic usage and function based on the real world experience and feedback from the system. The large power button provides clear affordance for the users.

One last main function button is the education part, where users can ask LLM about the information of scams. Three main function buttons keep the consistency of style. There are always a button to go back to a page in order to prevent errors like misclicking. The main page has the most main functions which consider the flexibility and efficiency to use. We reduced the number of functions to six so that it contains the aesthetic and minimalist design. For the report button, the user feedback channel is also a significant part for users to involve the design process. It also helps users to deal with the errors. The help function is inside the setting page, which gives users a way to get help from the help documentation.

7 USER TESTING & FEEDBACK

When we presented the Figma version of 365 Security Guard, it was appreciated for its clarity of scam warnings. But we received complaints about the lack of immediate feedback which hindered the user navigation. The

color-coded scam alerts helped the users distinguish the level of threat and demonstrated, corresponding to the cognitive load theory. While the deal check tool received positive comments for its quick response and voice recognition feature. Several users mentioned that our voice recognition could be enhanced in future stages to help them to avoid voicemail scams and phone call scams.

Our Figma also needs major improvement on user navigation and guidance. The initial Figma lacked immediate feedback for user actions, some buttons did not provide clear confirmation, leaving users unsure if their action has been captured. Many users mentioned this in their feedback sheet, stating that we could improve immediate feedback to shape a smoother navigation through the tool. We should reconsider button selections to ensure seamless screen transitions.

Picking up the key refinements to enhance usability, the team ensured that all of our spam notifications came with a brief explanation. To address the concerns for accessibility and inclusivity, we introduced dark mode, font size customization, as well as language preference. We paid extra attention to bring immediate feedback to user activity, by selecting buttons and control keys that would be shaded or colored once they are triggered, users claimed that navigation has significantly become easier. Moving forward, we plan to disperse our prototype to a broader audience in hopes to collect more feedback, ensuring that 365 Security Guard would get better day by day.

8 DISCUSSION & REFLECTION

We focus on student users highlights how important this specific capability. Key to our methodology is empowering students. Many students are faced with financial instability and might not be familiar with how to handle themselves in a scam. Our software stands out among traditional security software by providing a support mechanism after an attack has taken place, instead of merely providing preventive protection in advance. Traditional security software might block access to scam sites or alert users to suspicious messages, but they rarely provide help after a breach. By making recovery easier for students, 365 Security Guard is more than a prevention tool—instead, it is a proactive ally in online activity.

Reflecting on the development process made it clear that technical innovation alone was not enough; instead, user empowerment and empathy became the vital elements. This process highlighted the imperative to merge technical solutions with emotional intelligence. We witnessed firsthand how a carefully crafted tool could turn a daunting experience into an achievable recovery path. In summary, One-Click Recovery not only differentiates 365 Security Guard from other products on the market but also has a profound impact on users by restoring control and bringing hope after a scam. This reflection affirms our belief that antivirus software is designed to play both protective and empowering functions。

9 FUTURE WORK

We aim to further enhance the One-Click Recovery feature to be more robust and tailored to various scam scenarios. This includes the introduction of platform-specific dispute templates for a range of services like banking, payment apps, and e-commerce sites, so that the system can automatically prepare appropriate refund requests or reports. In addition, smart detection of the platform involved in a scam will allow the recovery process to automatically adjust itself. We also foresee an AI-powered recovery success predictor that analyzes past cases to estimate the likelihood of fund recovery, thus preparing users with realistic expectations and suggestions on best strategies.

The incorporation of support services in scam recovery is not limited to financial recovery; it has deep emotional repercussions. In future projects, 365 Security Guard has the capability to provide users with connections to mental health experts or school counselors to aid in recovery. After helping a student report a scam, the tool can offer a counseling session or stress management methods. By providing access to these support systems, the tool is showing consideration for the individuals' welfare that is wider than financial welfare, and this can lead to emotional recovery and restored trust.

Our aim is to make sure that tool is appealing to young users across different backgrounds. This means streamlining the user interface design to make it modern, intuitive, and appealing. We are considering having gamification features like dispensing badges or points for safe online practices and interactive tests to make learning about security enjoyable. We hope for students to not only use it actively but also to share it with others.

10 PEER RATING

Tianren Chen: 17% – Contributed to user research, survey design, report writing, Figma design, and Final Report.
Qingyue Yang: 17% – Contributed to UI design, Figma prototyping, presentation slides, and writing and formatting of IPD, UDP, and Final Report.
Ryan Liao: 17% – User testing, scam recovery feature development.
Lily Hu: 17% – User interview, comparative analysis, video editing, Figma design.

Chenghao Wu: 16% – Literature review, AI model research, discussion section.
Yanming Luo: 16% – Literature review, AI model research, discussion section.

11 REFERENCES

[1] 356 Security Guard, "365 Project User Research," Mar,02,2025 ,https://docs.google.com/document/d/1Qb7RKnhW4TI8LxflyRSFF571Q5fcPB5B1SquB7PvWVU/edit?usp=sharing

[2] 356 Security Guard, "365 Mid-Fi Protocol Type App By Figma," Feb,16,2025, https://www.figma.com/design/pQUtvxHxVDzK79foxxOqlt/ECS164---Final?node-id=0-1&p=f&t=WN0wbwTlE6W2pXUl-0