

SwindleSpotter – Group 2

Project Team Members

1. **Summary /Conclusion Writer & Overall Editor:** Brayden Waiters
 2. **Market Researcher:** Will Amey
 3. **Product Designer:** Ziheng Lei
 4. **Devil's Advocate/Critic/"Jack of all Trades":** Caleb Harsche
- ***Note: If you only have 3 members, then everyone will need to assume a part of the role of "Devil's Advocate/Critic/Jack of All Trades"***
 - ***If you have 5 members, there can be TWO people in the "Devil's Advocate/Critic/Jack of All Trades" role***
-

1. Executive Summary (Overview)

Welcome to our "Swindle Spotter" application proposal. With this app, you will be provided with automatic and secure AI protection from common online threats. This includes not only financial and informational scams through messages, emails, website links, or other harmful programs, but unlike every other security app, such as McAfee or Google's automatic detectors, we also protect users from social scams that have potential for real, physical harm, such as catfishing or suspicious activity. This is the perfect wall of defense for those who frequent online spaces, whether they're working, shopping, dating, or just trying to meet new people, they will feel an extra level of safety with "Swindle Spotter" installed. They can go about their daily business with no fear of targeted attacks resulting in money or information stolen, or dangerous encounters with online strangers.

Just a few of the features of our app include safety ratings of unfamiliar links, downloads, emails, and messages, and automatic background checks of all profiles found online, detecting contradictions, patterns, or suspicious activity in their interactions. And if this wasn't enough to convince you of the need for our app, everything you need is right here in this document.

2. Market Research and Need Justification

Swindle Spotter enters the market of scam detection services at a tumultuous time, as AI advances everyday, more and more companies are starting to use AI to detect scams. The amount of people who have been scammed or attacked online has skyrocketed in recent years.

Big tech companies such as Google, Meta, and Microsoft have been attempting to stop online scams for years, and with the help of artificial intelligence, they seem to have found a good way to do that. An example of that practice is with Google, they recently implemented their own AI powered fraud detection on Android devices to put a stop to scams that attack through phone calls and text messages.(*Google Online Security Blog*, 4 Mar. 2025) This clearly showcases a demand for scam prevention for consumers and the increasing prevalence of AI in modern technology, but is the AI these companies frequently use really that helpful

3. Product Description

Swindle Spotter is a frame app that works with other messaging apps and appears as a floating window within the chat interface. When you receive an unfamiliar message, Swindle Spotter automatically checks the website's certificate and security, alerting you by changing the website link to red (100% scam), yellow (50% scam), or green (appears safe).

In addition, if you're unsure about the website's safety, Swindle Spotter can also create a fake mobile frame on your phone to prevent dangerous behaviors like information collection, pop-up ads, forced downloads of unknown viruses, and inaccessible login attempts.

We've also added a history system. When a website Swindle Spotter deems safe appears again, Swindle Spotter's AI will identify it and automatically color-code the link. Even if a fraudulent website simply changes its domain name or slightly modifies its website name, Swindle Spotter will still recognize it and display a question mark button above the website. Clicking the changed letters will also highlight the link.

Furthermore, we often receive text scams on social media apps from strangers asking questions like "How are you doing?", "Needing ID verification?", or "Your package has been detained." Swindle Spotter, an AI-powered app, uses big data to determine if a message is likely a scam, prompting users to be cautious or block them. If the people sending this message are the user's friends, Swindle Spotter won't automatically detect scams unless the user requests it. However, due to history settings, scams encountered will be flagged and displayed with a question mark to the right of the message. Swindle Spotter will explain the scams to users and raise awareness.

Swindle Spotter is suitable for anyone who enjoys finding resources online, whether it's e-books, images, or videos. Scam websites and free, public websites often have the same name but different domains. Can you find the right website without being sure? For example, Zlibrary is a free and publicly available e-book website, but numerous fraudulent websites use the same name: z-lib.cc; z-lib.ai; z-lib.id; z-lib.sk. Only one of these URLs is correct, and the framework and

settings are identical. Scammers use various legitimate reasons, such as memberships, donations, and premium versions, to scam you.

Swindle Spotter is also suitable for seniors who need to use their phones (to prevent pension scams, "how are you doing" scams, and scams requiring identity verification). Simply download the app and agree to permissions like pop-up notifications, and it will automatically run in the background. It will automatically pop up and alert seniors when a link or unfamiliar message appears, detecting danger and alerting them.

Online sellers and buyers can also use it to prevent fake links (avoid misleading links like "Click the link to get a free phone"), or anyone tired of spam and scams.

4. Possible Issues and Counterarguments

The safety concerns are not addressed on how this app will possibly steal other people's information and most likely sell it to shady companies. Therefore people will start not trusting this app enough to download it and the app will most likely tank in sales but we can assure you that this is a safe app and we will use a trained team of people in order to make sure that what a customer sends is a scam or not. What happens when a person doesn't consent to having their private conversations viewed at and put out for all the employees working on this app to see, who manages what the employees see and don't see and I have the answer to that question, we will have a moral consultant to make sure everyone is doing right by honesty and integrity %100 of the time and if they don't uphold this level of integrity they will be immediately fired.

This app could potentially gain access to every private email, text, and search history, and the company could be hacked, getting your private information accessed by people all over the world, but I can assure you that this company pays for the top cybersecurity specialists in the world and it will be a very hard task to hack into this company. People might say that the market for this kind of app is oversaturated and that there are too many apps like this in the world that just all do the same thing. While I can agree that this market is very saturated and there are a million different apps you could use for this kind of thing, our app will specifically target the signs of phishing and scams by having a aforementioned team of people, not AI, making sure that every single detail in a profile on Tinder, or random text that includes a random link to somewhere unknown, the Swindle Spotter app will detect all of that and no AI will be used to make sure that no mistake is made, very rarely does an app not use AI to detect these kinds of things and instead a full team of people to make sure you don't get scammed or hung up on and drained of your money by a suspicious Tinder profile.

Now you might ask “why don’t I just be careful on the internet and double check everything before I make a conclusion?” What I answer to this question is that scammers are adapting like chameleons and it is getting harder to try and find out who is and isn’t a person waiting to take all your money, assets, and identity away from you without you even knowing until it’s too late. That’s why it’s really important to have people who are equipped to spot these scams and know the difference between real and fake, not a lot of app companies for this business can say that they do this. Now it is really unethical to access other peoples personal information but that would only be required if we are looking at vishing, Tinder scams only require the profile so there will be a waiver to say that you consent to reading your texts, messages and emails or you don’t and we only use this for spotting catfishing on Tinder and anything else that doesn’t require us reading about your private life.

I feel that this app called Swindle Spotter can help eliminate all the scams in the world, making them completely obsolete and drive out the entire scamming business due to this app actively sensing and making sure no one gets scammed so no one who didn’t earn their money in this society doesn’t get any money.

5. Conclusion and Recommendations

With your support, we will launch an impactful and necessary product for our modern, online world. Everyday internet users will be safe from various attacks, scams, and programs that could potentially put their livelihood, or even lives, at risk. By detecting suspicious patterns and communicating with the user via safety ratings, these scams will become minimized to a point where they’re ineffective. That way, people all across the world can freely use and interact with the vast tool that is the online world without harm. Investment in our application is investing in changing our ever-evolving world for the better. So share your support for “Swindle Spotter”!

6. Appendix

Roughly three-quarters of Americans have experienced an online scam or attack

% of U.S. adults who say each of the following has happened to them



Note: "Bought an item online that was counterfeit or never arrived and wasn't refunded" was originally asked as two separate items; that figure includes those who say either or both has happened. Those who did not give an answer are not shown. Please refer to the questionnaire for full question wording.

Source: Survey of U.S. adults conducted April 14-20, 2025.

"Online Scams and Attacks in America Today"

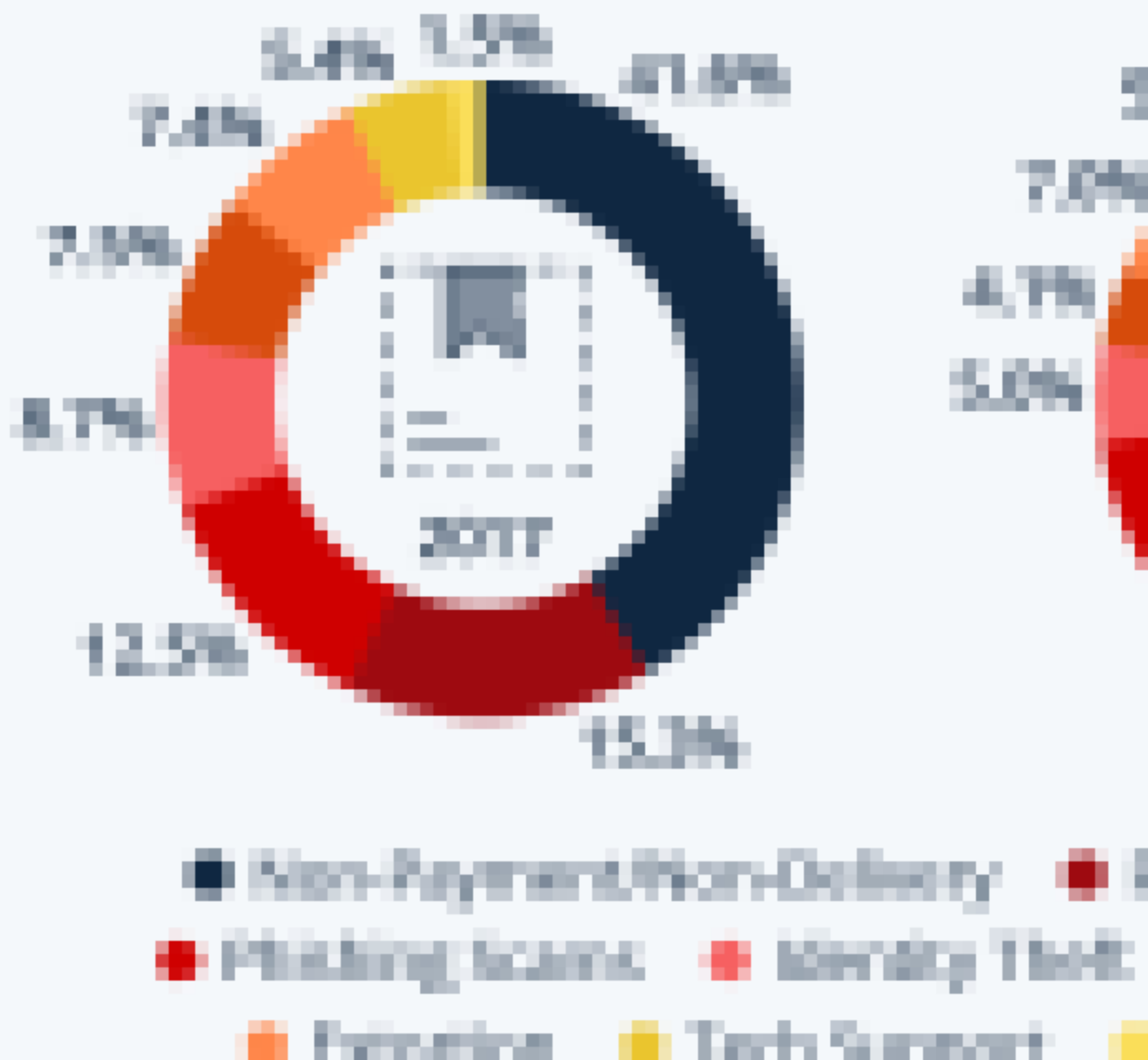
PEW RESEARCH CENTER

[Attacks in America Today | Pew Research Center](#)

(Source: [Online Scams and](#)

The Most Prevalent of Cyber Crime

Share of worldwide cyber attacks by type



(Source:https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/?srltid=AfmBOor95CMR0xx844OLBDAoiksWPO9Qwv_S064ANLdKHQ6J_AQQM7I)