Proposal for Group 4

Title: Fried Phish

Project Team Members

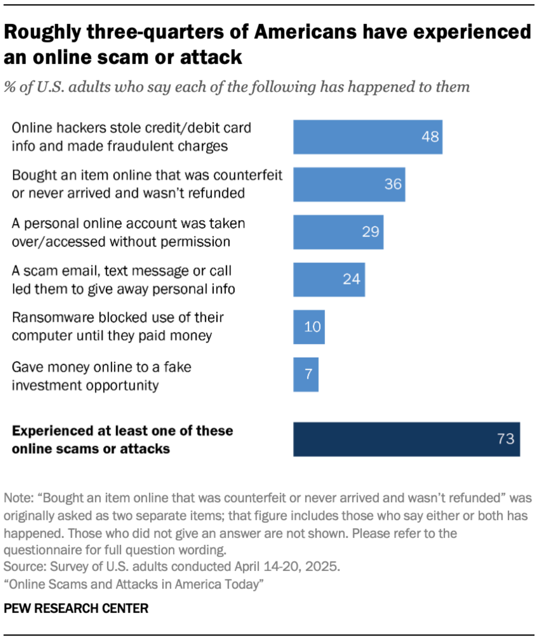
1. **Summary/Conclusion Writer & Overall Editor**: Alex Kelly
2. **Market Researcher**: Alex Kelly
3. **Product Designer**: Xander Tidrick
4. **Devil's Advocate/Critic/"Jack of all Trades"**: Jai Rafael Gallardo

1. Executive Summary (Overview)

Fried Phish is a product that aims to assist the everyday internet user in avoiding scams that can steal their data, compromise their accounts, or allow a malicious individual to steal their identity. Our product is a computer extension that runs in the background of your computer, alerting the user when they are at risk of clicking on a scam ad, email, or a fishy link on *any* chat app, browser, email system, social media platform, and more! Fried Phish utilizes revolutionary Artificial Intelligence technology that detects scams in real-time by harnessing a vast dataset of known scams to predict potential scams.

With FriedPhish, people young and old can be saved from scams that they may not even know they are facing. As our application is simply an extension for your computer, it can be easily installed and used by people with most types of computers. Our product can cater to a very wide audience as well, as individuals, young, old, and anything in between can use FriedPhish and benefit from it. Frankly, it would do people a disservice not to install it!

2. Market Research and Need Analysis



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

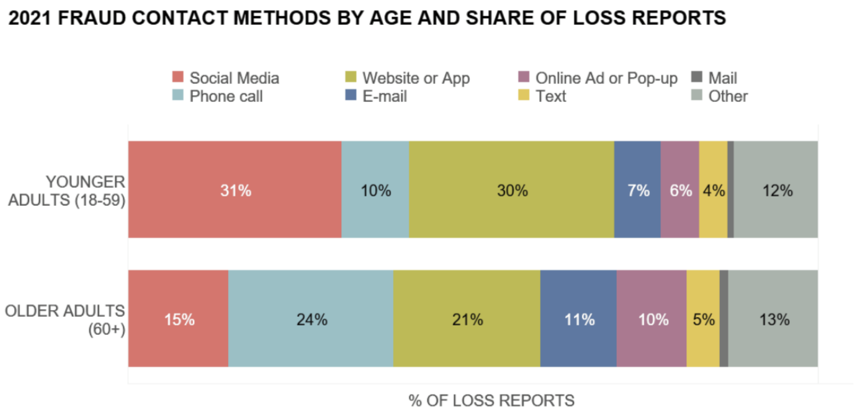
% of U.S. adults who say each of the following has happened to them

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

(Pew Research Center, 2025)

In the United States, up to 73% of people have fallen victim to an online scam, according to the Pew Research Center. Along with this, 29% of people have had their personal online accounts taken over without permission, and 24% percent of people have given away personal info by accident via a scam email, text message, or call. In addition to this, the vast majority of fraud in the United States starts on the internet. According to the FTC, in a graph shown below, younger individuals (18-59 years of age) are more likely to fall victim to a scam on social media, while older individuals (60+ years of age) are more likely to fall for a scam on a phone call or website. This presents a significant vacuum in the need for prevention tools against scams, as many people across a range of ages are susceptible, regardless of age.



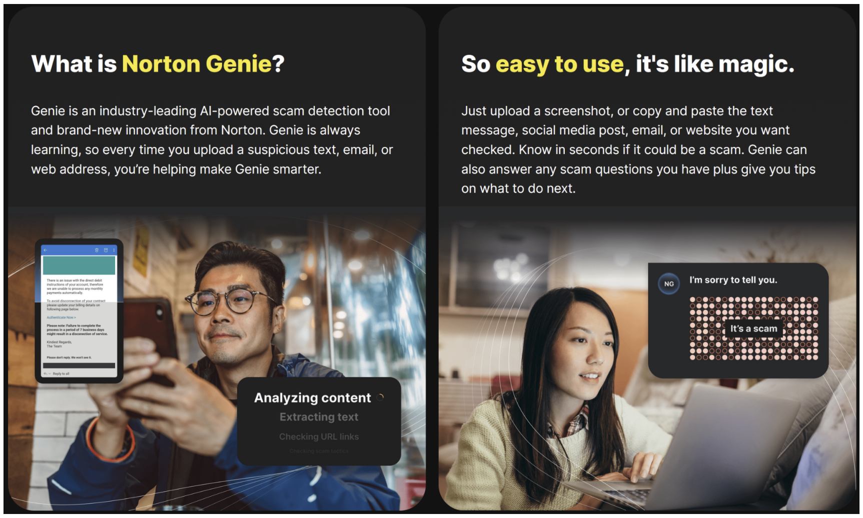
2021 FRAUD CONTACT METHODS BY AGE AND SHARE OF LOSS REPORTS

Figures are based on fraud reports to the FTC's Consumer Sentinel Network that indicated a dollar loss, including reports provided by data contributors. Reports without age and contact method data are excluded from percentage calculations.

(Federal Trade Commission, 2022)

While there is strong representation for other virtual risks like antivirus programs, there are fewer direct resources to prevent people from clicking on scam links in emails or on the internet. One resource that does exist in the current market is a program called Norton Genie. This program allows users to input items such as social media posts, emails, or websites they believe are scams, and Norton's “AI” detects whether the item is considered to be a scam or not. This solution is a standalone application, while our product aims to be integrated with web browsers, social media platforms, email, and more to directly detect scams as you go about your internet business.

Example of Competitor Product (Norton Genie)



What is Norton Genie?

Genie is an industry-leading AI-powered scam detection tool and brand-new innovation from Norton. Genie is always learning, so every time you upload a suspicious text, email, or web address, you're helping make Genie smarter.

So easy to use, it's like magic.

Just upload a screenshot, or copy and paste the text message, social media post, email, or website you want checked. Know in seconds if it could be a scam. Genie can also answer any scam questions you have plus give you tips on what to do next.

(Norton, 2025)

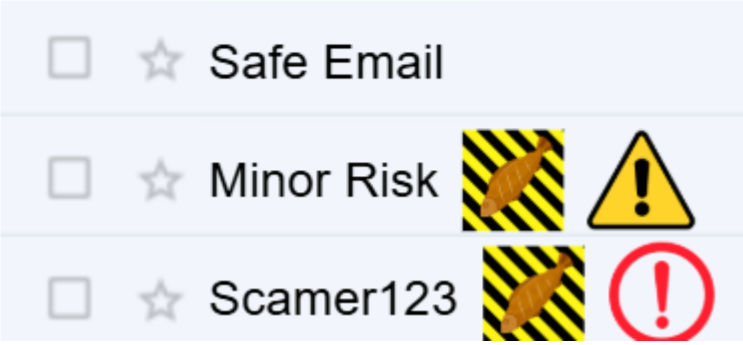
3. Product Description

Fried Phish is intended to be extremely easy to use and understand, with minimal user input necessary to function, while having many customization options to improve the quality of the user’s experience. The notices and alerts for the user when a potential scam or virus has been detected have been made with the intention of being obvious so they are extremely difficult to miss, as they are large and located right next to the message, email, or web link that the user is looking at. On top of that, Fried Phish is able to be accessed and used on all search engines and messaging apps.

There are three different outcomes when Fried Phish scans an email or website. The first outcome is having no alert when Fried Phish detects that there isn’t any potential that the email or website could be harmful to the user. The second outcome happens when Fried Phish detects that the email or website is asking to verify personal information, like creating an account, that could potentially have some security issues or is a potential threat to the user's data. Fried Phish then provides a mellow but obvious warning to ensure that the user is notified of the potential dangers from interaction with the email or website. The third outcome happens when Fried Phish is almost certain that the email or website has major risks to the user's data and should be avoided at all costs. Fried Phish will provide several obvious warnings to the user notifying them of the security problems and provide the proper solution on how to deal with the scam or virus.

Additionally, Fried Phish also has several customizable options that allow users to optimize their experience with Fried Phish. If the user is receives emails from a source that the user knows is reliable, or uses frequently, but Fried Phish keeps flagging them as potentially problematic, they are able to utilize Fried Phish's whitelist feature, where the application will not check any emails or websites that are on the whitelist. Likewise, Fried Phish also has an option to blacklist certain emails or websites, so Fried Phish will automatically flag them. Both the whitelist and blacklist features of Fried Phish are for personal preference and quality of life. If the user thinks that Fried Phish is flagging or missing things it shouldn't be, there will be the option to report it when whitelisting or blacklisting the web site or message respectively to improve the product for all users. Most of Fried Phish's features can be turned on and off. Fried Phish has different features for disabling it for checking emails and checking websites or links in the search engine. If the user only wants to use Fried Phish for checking email, they are able to only allow Fried Phish to access their emails and not anything else on their web browser. The Fried Phish extension is able to be accessed and used on all search engines and messaging apps, like Gmail, FireFox, Discord, Facebook, ect., with the option to enable and disable it separately on each one.

Fried Phish separates itself from other scam protectors by utilizing AI to quickly search emails, messages, and the web for problematic websites, links, or scams. Because of this, Fried Phish doesn't need to store and collect user data like other scam protectors to work efficiently. Users will have the ability to let Fried Phish save information on data it has already scanned for slightly better performance and to help train and improve our AI, but this setting will be off by default in respect of our users.



☐ ☆ Safe Email

☐ ☆ Minor Risk ⚠

☐ ☆ Scamer123 ❗

Created with Canva by Xander

4. Possible Issues and Counterarguments

One of the main challenges that could arise would be privacy and security concerns. The extension would need to view the person's email and its contents to accurately detect if the email is a scam. It would also check messaging applications like Discord. The product would also need to learn from the emails and messages that come in, in order to detect scams. We would ensure our customers that we would keep their data in secure servers backed with multiple firewalls. We would never sell customer data to third parties, as we view this as wrong. The data collection will only be used by us, not to spy on our customers, but to learn how scammers are improving their tactics and to streamline legitimate emails to the customer without unnecessary flagging.

Another challenge would be accuracy. False positives, which if too many happen, would cause the user to become annoyed and disable the extension. The product could also give false negatives, which would cause the user to fall for the scam and completely distrust the product as a whole. These misleading flags would be solved through our AI model, which would undergo months of vigorous testing to strengthen its detection capabilities and effectiveness. We understand that not everything is made perfectly and some errors may occur, which is why the user has the ability to flag these false positives/negatives to further strengthen our AI. This feedback would be directly given to the AI, adding to what it already knows. Our AI would have the capability to detect the scamming tactics that go on in our ever-developing world.

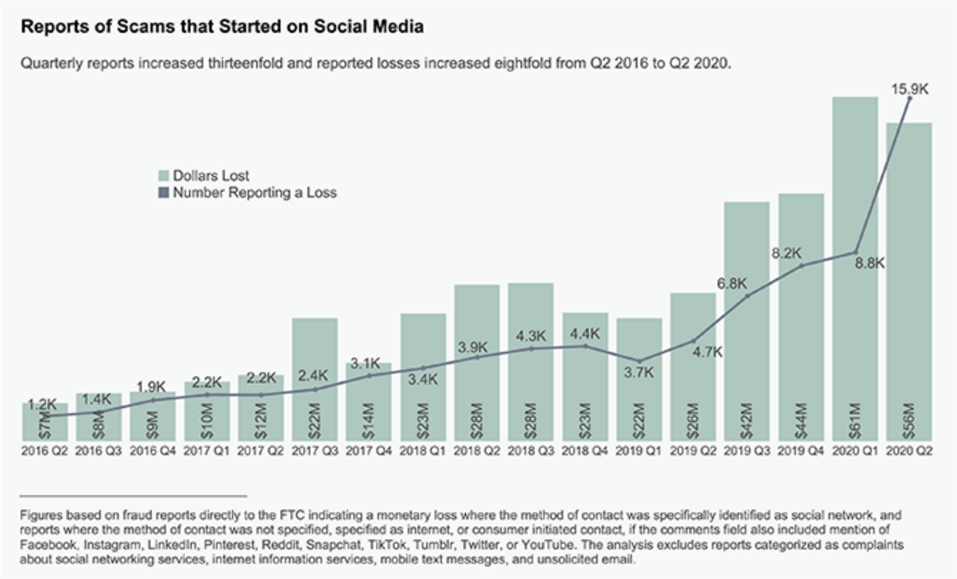
Other challenges include product differentiation. People might wonder how our extension is different from other scam detectors already on the market. Solutions to that problem would be our creative and distinct logo and name. Our AI model would be one of the strongest on the market. We would need a lot of testing and verified reviews from our clients to build our credibility. Another potential issue would be our use of AI. While some people disagree with the use of AI, we believe that it is very valuable in this application. The use of AI allows the extension to continuously learn and adapt to the constantly changing methods used by scammers, providing customers with the reliable protection they deserve.

5. Conclusion and Recommendations

FriedPhish is an essential part of the modern web user experience. With scams being an extremely prevalent method to steal from people digitally, tools like FriedPhish are essential in stopping these scams in their tracks. In practice, FriedPhish will save users thousands of dollars in potential losses from hackers stealing their financial or personal information, all in one extension.

With FriedPhish being a lightweight and easy-to-use extension, people from all walks of life can easily access and use our product, potentially preventing them from falling victim to an increasingly hostile online world. We strongly recommend moving forward with the development of this app, as it can benefit a wide variety of people in a simple and affordable way. Going forward, our team plans on continuing development of this application and releasing it to a wide range of users who would benefit from it.

6. Appendix



Reports of Scams that Started on Social Media

Quarterly reports increased thirteenfold and reported losses increased eightfold from Q2 2016 to Q2 2020.

Figures based on fraud reports directly to the FTC indicating a monetary loss where the method of contact was specifically identified as social network, and reports where the method of contact was not specified, specified as internet, or consumer initiated contact, if the comments field also included mention of Facebook, Instagram, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Tumblr, Twitter, or YouTube. The analysis excludes reports categorized as complaints about social networking services, internet information services, mobile text messages, and unsolicited email.

(Federal Trade Commission, 2020)

Anderson, Jeffrey Gottfried, Eugenie Park and Monica. “Online Scams and Attacks in America Today.” *Pew Research Center*, 31 Jul. 2025, https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/.

International, Fraudcom. “Data Security and Privacy as Pillars of Fraud Prevention.” *Fraud.Com*, 19 Jul. 2024, https://www.fraud.com/post/data-security-and-privacy.

ThreatMark. “Why Traditional Fraud Prevention Measures Are Ineffective Against Modern Fraud.” *About Fraud*, 7 Nov. 2024, https://www.about-fraud.com/why-traditional-fraud-prevention-measures-are-ineffective-against-modern-fraud/.

Free Scam Detector - Prevent Phishing Scams - Genie by Norton. https://us.norton.com/products/genie-scam-detector. Accessed 16 Sep. 2025.

“Who Experiences Scams? A Story for All Ages.” *Federal Trade Commission*, 9 Nov. 2022, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages.

“Scams Starting on Social Media Proliferate in Early 2020.” *Federal Trade Commission*, 21 Oct. 2020, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020.