Proposal for Fried Phish

Title: Fried Phish

Alex Kelly, Xander Tidrick, Jai Rafael Gallardo

1. **Summary/Conclusion Writer & Overall Editor**: Requires concise writing and a holistic understanding of the project.
2. **Market Researcher**: Requires skills in research and data interpretation.
3. **Product Designer**: Requires technical knowledge and creativity.
4. **Devil's Advocate/Critic/"Jack of all Trades"**: Requires critical thinking and the ability to construct persuasive arguments. This person will also assist the other 3 team members with their responsibilities as needed.

---

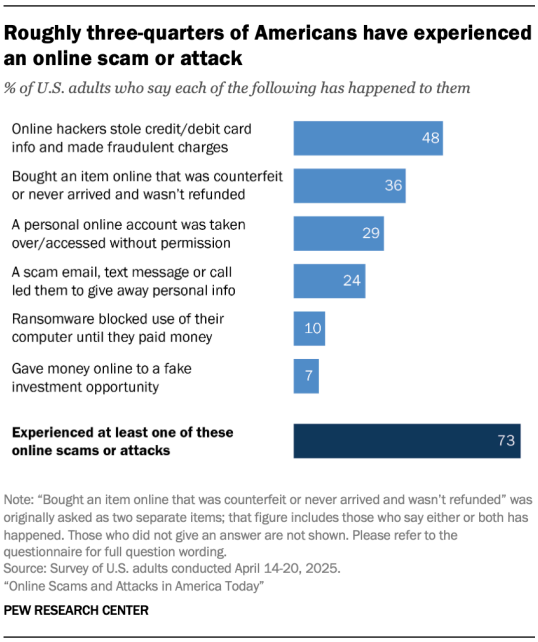
1. Executive Summary (Overview)

Fried Phish is a product that aims to assist the everyday internet user avoid scams that can steal their data, compromise their accounts, or allow a malicious individual to steal their identity. Our product is a browser extension that runs in the background of internet browsing sessions, but alerts the user when they are at risk of clicking on a scam ad, email, or a fishy link. It uses revolutionary Artificial Intelligence technology that detects scams in real time by harnessing a vast dataset of known scams in order to predict what may be a scam.

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 a lightweight brower extension, it can be easily installed and used by people with most types of computer. 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 installing it!

---

2. Market Research and Need Analysis

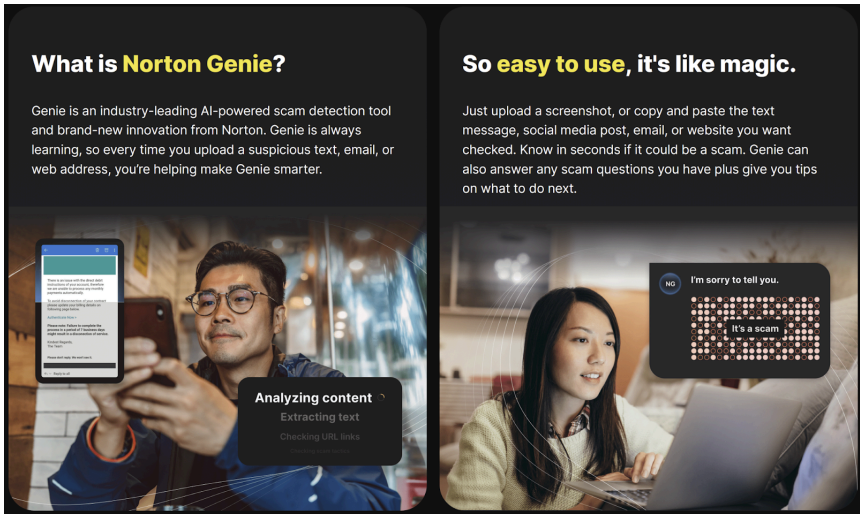


(Pew Research Center, 2025)

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. This presents a significant vacuum in the need for prevention tools against scams.

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 to more directly detect scams as you go about your web browsing.

Example of Competitor Product (Norton Genie)



(Norton, 2025)

---

3. Product Description

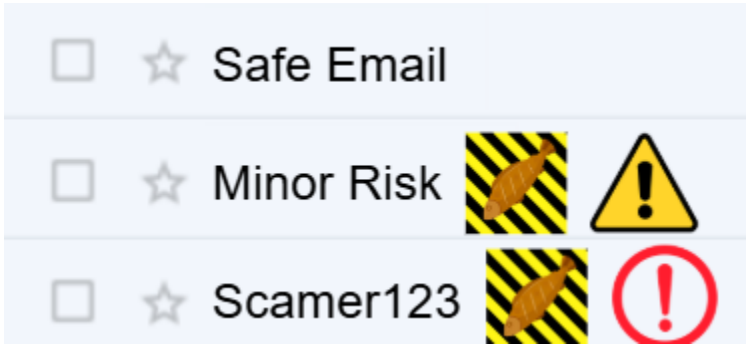
Fried Phish is intended to be extremely easy to use and understand, with minimal user input necessary to function, while having many customization options to improve the quality of the user's experience. The notices and alerts for the user when a potential scam or virus has been detected have been made with the intention of being obvious so they are extremely difficult to miss.

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 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. 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 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.



Created with Canva by Xander

4. Possible Issues and Counterarguments

One of the main challenges that could pop up would be a privacy/security issue. The extension would need to view the person's email and its contents to accurately detect if the email is a scam or not. The product would also need to machine learn off of the emails that come in, in order to tell if said email is a scam or not. There would also be the problem of 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 as well which would cause the user to fall for the scam and completely distrust the product as a whole.

Some other problems that could arise are the product differentiality. People might wonder what is the difference between our product and other scam detectors on the market. We would need a lot of testing and backed up reviews for our clients to begin having our product as a thought to solve their problems. Another possible issue would be our use of AI due to the fact that lots of people disagree with the use of AI even though it would be very useful in this application.

---

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 browser extension.

With FriedPhish being a lightweight and easy to use browser extention, 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.

---

6. Appendix

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/.