Project 2I, Report

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

Scam Prevention

Team Members

Sam Hutcherson - Performed contextual inquiry, sketched some of the designs and a storyboard, helped write project submissions, presented the project
Justin Pirman - Performed an interview with the BofA employee, helped with the initial design and with the storyboards.
Jose Becerril - Worked on Proposed Designed Sketches, helped write final report
Chase Wallendorff - Conducted an interview with a scam victim, helped with initial designs and storyboards, helped plan and prep throughout the project

Problem and Service 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 conceptualized 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.

Design Research Goals, Stakeholders, and Participants

The goal of our design research was to gain a better understanding of scams on a large scale: what kind of scams are out there, how some people might be susceptible to them, how some people are able to protect themselves from them, how scammers are able to successfully conduct their work, how security specialists work to keep people safe, and so on. We weren't just concerned with gathering information from a single side of a scam, but from all angles that exist in these interactions. Our design research included three separate investigations into our problem space,

Interview 1, Cybersecurity Specialist

Though wishing to remain anonymous in name, the cybersecurity specialist we interviewed allowed us to share that they work for BofA (Bank of America) and have a degree in computer science, with a focus on cybersecurity. We interviewed them over facetime, where we discussed a lot of issues that are pertinent to scams in cyberspace. Since they had some time to spare and a wealth of information to share, we figured an interview was the best research method for this participant.

Interviewing a cybersecurity specialist seemed like the perfect opportunity to gather some good information for our problem space, since their entire domain revolves around scams and security. From this interview, we gained a lot of professional-grade knowledge on the world of cyber scams, the most important being that education and caution are the most effective defense against them.

Contextual Inquiry, SIUE Student

T.J. is a fourth-year mechanical engineering student at SIUE. The contextual inquiry took place in his apartment, where we looked at his system for dealing with scams and protecting his information digitally. We knew T.J. would be a suitable candidate to include in our design research since, as a student attending the university, we knew he would have to deal with scam attempts relatively often. Since T.J. is a busy fourth-year student at the university, we figured contextual inquiry (with a bit more lean to "fly on the wall") was the best way to gather information from this participant.

Our observation of T.J's system for tackling this issue gave us some great insights - though T.J. receives what many might consider to be a high number of scam emails, he falls prey to none of them because he is aware of the prevalence of scams and knows how to spot them when they come his way.

Interview 2, Scam Victim

Our scam victim, Victor, is a 62 year old ex-engineer for Boeing. We interviewed him following a scam he fell for about four weeks ago. In this scam, Victor was contacted by an individual claiming to be from the IRS, demanding payment. Since he had an open afternoon, we figured an interview would be good.

We chose to interview Victor because we saw it as a great opportunity to learn what a scam could look like from the side of the victim. From this interview, we learned what it can look like when a potential victim is contacted by a scammer, what they might be told to do, and what can happen from there.

Design Research Results and Themes

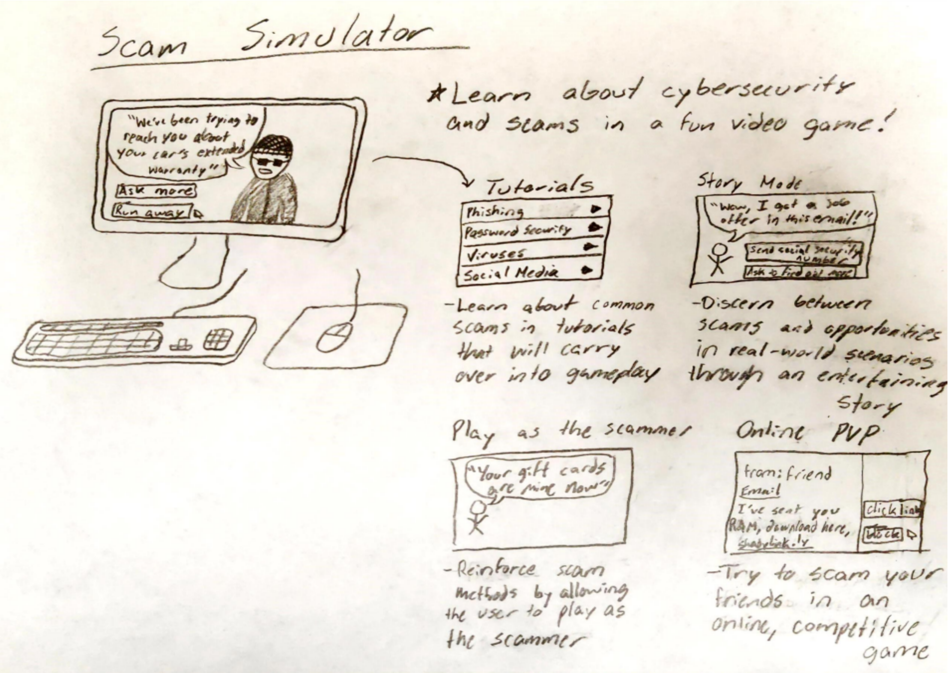
We found that the most common scams that people encounter are via messaging or email, such as the IRS fraud scam, malware scams, or fake job postings. Almost all scam messages come from a person acting as an authority figure, and the harsher ones come with a time limit to respond. This type of scenario can pressure people to make a decision quickly, and this can have disastrous results.

Another theme that we found is that those who are educated about scams are much less likely to fall for them. However, this does not mean that they are unbothered by scams. Two of our research participants were well-educated in the different types of scams, so they were able to avoid falling for them. However, they still receive scam emails, which can be annoying to deal with. Our third participant had fallen for a scam without even realizing it until he was notified by someone that was able to recognize the scam. If Victor had encountered this type of scam before and was able to recognize it, then he would not have fallen for it. It really is a matter of recognizing a scam to be able to avoid it.

These two ideas had the largest influence on our designs. Our solution needs to make the user aware of the scam, and it needs to do this quickly so that the user does not have time to react and fall for the scam.

Proposed Design Sketches

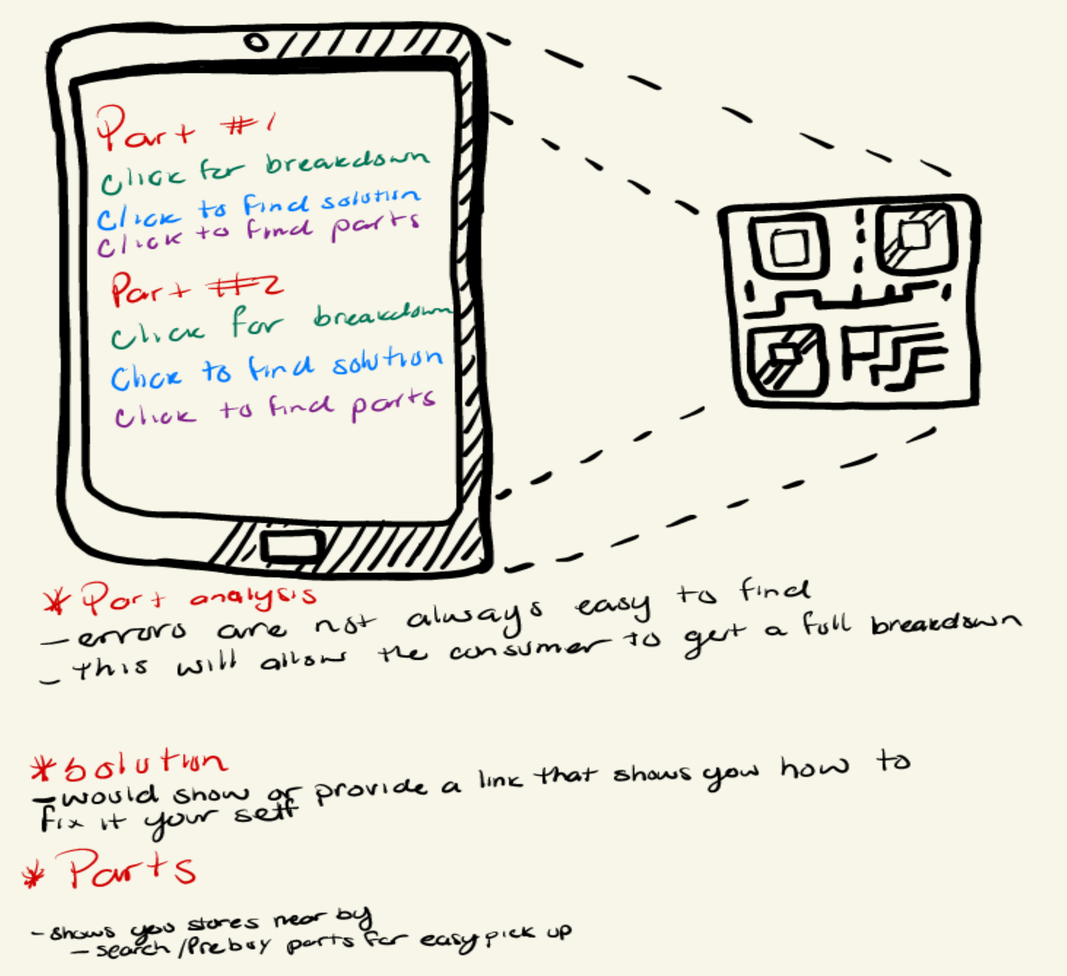
Design #1: Scam simulator


Scam Simulator
"We've been trying to reach you about your car's extended warranty"
Ask more
Run away
★Learn about cybersecurity and scams in a fun video game!
Tutorials
Phishing
Password Security
Viruses
Social Media
-Learn about common scams in tutorials that will carry over into gameplay
Story Mode
"Wow, I got a job offer in this email!"
Send social security number
Ask to find out more
-Discern between scams and opportunities in real-world scenarios through an entertaining story
Play as the scammer
"Your gift cards are mine now"
-Reinforce scam methods by allowing the user to play as the scammer
Online PVP
from: friend
Email
I've sent you RAM, download here, shadylink.ly
click link
block
-Try to scam your friends in an online, competitive game

This tool allows the user to practice any type of scam from phone scams to another scam like the IRS is after you. This not only teaches but we believe engages the user more since is an interactive game as well, it will allow the user to be more aware of such scams and be more knowledgeable on how to approach any iffy emails or text messages since he/she will be presented with multiple scenarios to stop from getting scammed. This design supports our plan for many reasons, as we stated before this will enhance the awareness from many people varying from many ages, it will also provide real life scenarios to be more real life scams. We can pursue this further by adding more levels and making it more engaging so the user can stay engaged more and would come back the next day for a different challenge.

One of the many problems we encountered was how are we gonna maintain the attention of the user with the game we created. Many games that want to teach something like this are regarded as boring or just do not catch the attention of people. The other problem was if we do manage to bring the audience into the game, how are we going to keep them coming back. We came up with a few ideas that might work with the range of ages we are planning to play the game, the main two ideas was to have a small but yet interactive tutorial that will teach the different types of scams but have the user follow what scammers would do in such a scenario. The second mode was to have the roles flip, this would show if the user is really understanding how the scam works and the typical ways each scam is approached.

Design #2: Shopping App



*Port analysis
- errors are not always easy to find
- this will allow the consumer to get a full breakdown

*solution
- would show or provide a link that shows you how to Fix it your self

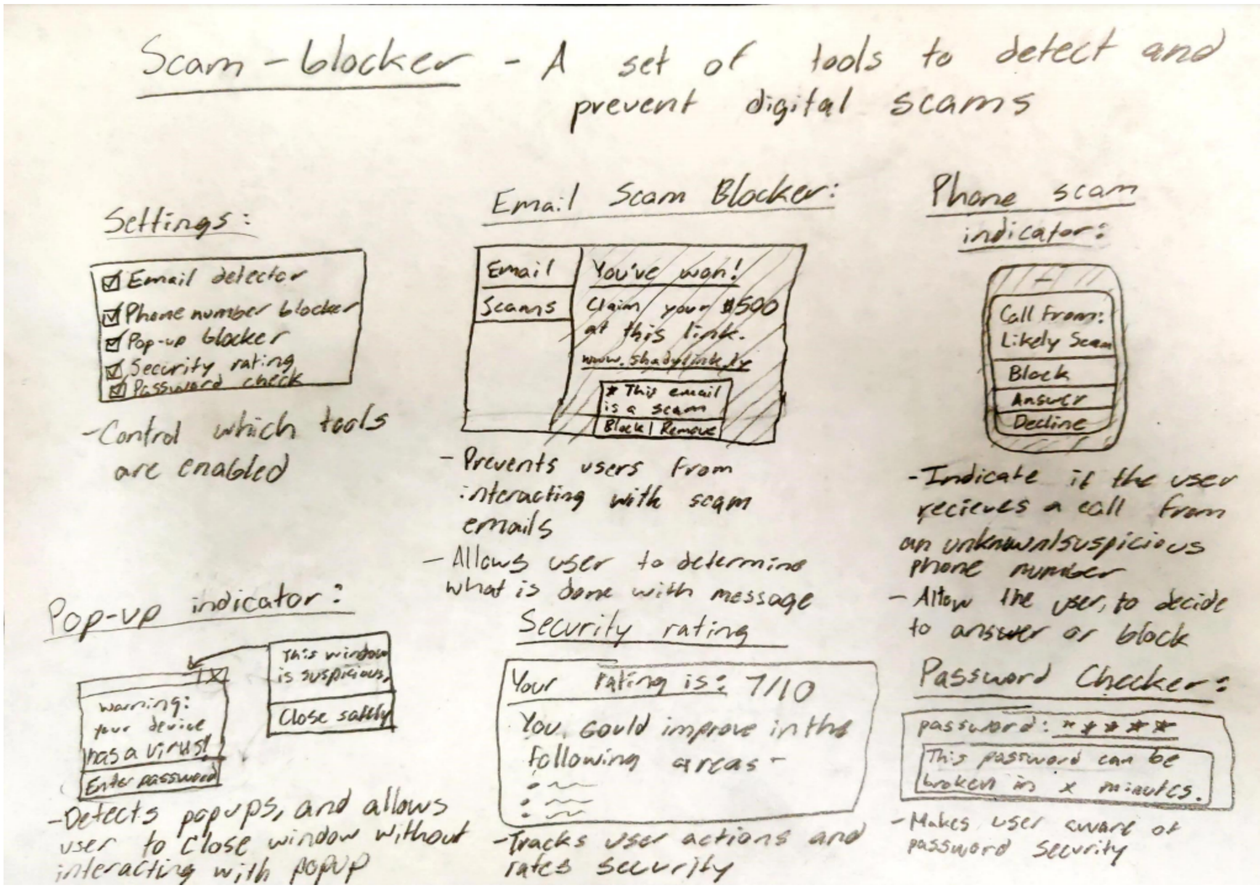
*Parts

- shows you stores near by
- search /Prebuy parts for easy pick up

For this design, we expanded on the idea of quickly educating the user about scams, in the area of shopping scams. This began with the idea of mechanics scamming regular people that may have little to no knowledge on how to fix a car, but later on we decided to broaden that idea and incorporate just about any product and give the consumer the option of watching a small video on how the product works and the average price is going on the market at that given moment.

This educates the consumer by showing them current pricing giving them a proper understanding of how to use it. This can be made better in the future to expand it not only for shopping but for various uses.

Design #3: Scam Blocker


Scam-blocker - A set of tools to detect and prevent digital scams
Settings:
☑ Email detector
☑ Phone number blocker
☑ Pop-up blocker
☑ Security rating
☑ Password check
-Control which tools are enabled
Email Scam Blocker:
Email
Scams
You've won!
Claim your $500 at this link.
www.shadylink.ly
* This email is a scam
Block | Remove
-Prevents users from interacting with scam emails
-Allows user to determine what is done with message
Phone scam indicator:
Call From: Likely Scam
Block
Answer
Decline
-Indicate if the user recieves a call from an unknown/suspicious phone number
-Allow the user, to decide to answer or block
Pop-up indicator:
☒
Warning: your device has a virus!
Enter password
This window is suspicious,
Close safely
-Detects popups, and allows user to close window without interacting with popup
Security rating
Your rating is: 7/10
You could improve in the following areas -
-Tracks user actions and rates security
Password Checker:
password: *****
This password can be broken in x minutes.
-Makes user aware of password security

This design allows the user to control what type of scam is getting blocked, not only stops them from replying to emails, phone calls/texts, and checking password security, with phone/ text scams it urges the user to practiced safe ways to approach a possible scam, not only it shows how to detect a link that is send through a text message. This supports our task for the same reason since it is teaching the user how to avoid scams but also offering a way to protect themselves in the future.

This design addresses the most scams in the least intrusive way, while handling these scams quickly. This solution best fits the themes of our design research, which is why we chose this design going forward.

Answers to Task Analysis Questions

Who is going to use the design?

Anyone that is bothered by scams, or needs help identifying scams can use our design. There is a wide audience, since our design can be used by anyone receiving scams.

What tasks do they now perform?

People need to identify scams, and then determine how to deal with them. This process is not always successful. Unfortunately, people need to be educated in the different types of scams in order to avoid them.

What tasks are desired?

Most people don't want to see any scams. If they do see scams, they would like to be able to identify them, and avoid receiving similar scams in the future.

How are the tasks learned?

These tasks can be taught by people that are aware of the different types of scams. This can be a lot of work since there are so many different kinds of scams. People have to be knowledgeable about technology as well.

Where are the tasks performed?

Scams are typically received via messages through email, phone, or social media. This means that most of the time, people have to address scams on their computer or phone. When scams are received on these devices, the user must recognize and remove these messages.

What is the relationship between the person and data?

People tend to be trusting of technology, which can make them susceptible to scams. People want to be able to use their device without worrying about being tricked into losing money. Even if the person is able to recognize scams, it's still annoying to receive these messages.

What other tools does the person have?

There are some apps that can be used to block robocalls, and many emails have spam filters, but both of these solutions are not always accurate, and can be intrusive on the user's experience. The best solution to deal with scams is to be able to recognize these scams, but even if a user is able to recognize a scam, they still have to deal with these messages by blocking or deleting them.

How do people communicate with each other?

People can communicate via email, phone, text, and social media. All of these places are susceptible to scams, and this can diminish the experience of communicating on these platforms.

How often are the tasks performed?

Every time a user receives a message, they have to check if the message is suspicious and determine if it is a scam. This happens multiple times a day. Obvious scams occur often as well, and can be received multiple times per week.

What are the time constraints on the tasks?

Most scams are designed to make the user act quickly. If the user does not identify the scam, they could lose their money in a matter of minutes. So the scam needs to be identified as soon as it is received, or the user should at least be made aware that the message is suspicious at the moment the message is received.

What happens when things go wrong?

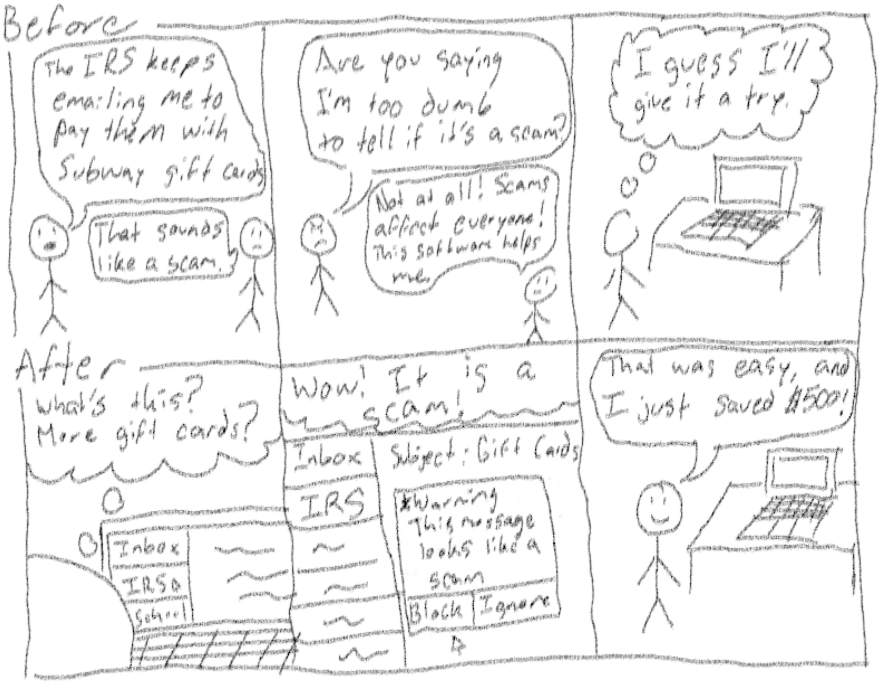
If a scam is not identified, it can result in identity theft or stolen money. Not to mention, the user may be embarrassed by falling for a scam. Most of the time, after the scam has been completed, the user is unable to get their money or information back.

Written Scenarios “4x5"

<u>Scenario 1:</u>

Frank is an overly caring person and is proud of his completely clean criminal record. He often gets messages from anonymous people online and finds it difficult to determine which are true and which are fraudulent. Recently he received a message from someone who claimed to be in the IRS and told him that he still had an overdue balance on his tax form. Frank has always remembered to file his taxes in a timely fashion and made sure the amounts all added up. This worried him since having the IRS convict him of tax evasion would destroy his perfect criminal record. The person on the other line said he had 24 hours to repay the debt or the IRS would come to his home and arrest him. The message stated that the only way he would be able to send the money safely to the agency would be to buy subway gift cards and give those codes to them over email. Frank immediately went to his local subway and bought a few hundred dollars in gift cards to pay what he thought was the IRS. When talking about it to his friend Tony, Tony realized that the person messaging Frank was not the IRS. Tony is much more aware of scams than Frank and warned him about the prevalence of scams. Frank took offense to what Tony said but it is unfortunately very common to fall for such a scam and that doesn’t make Frank dumb for not recognizing it was a scam. Frank then downloads our software by Tony’s recommendation and gets another message from a scammer attempting to take his money again. This time, the software recognizes that the message is from a fraudulent account and warns Frank to not send any money. Frank now can safely open messages without the fear of accidentally falling for another scam.

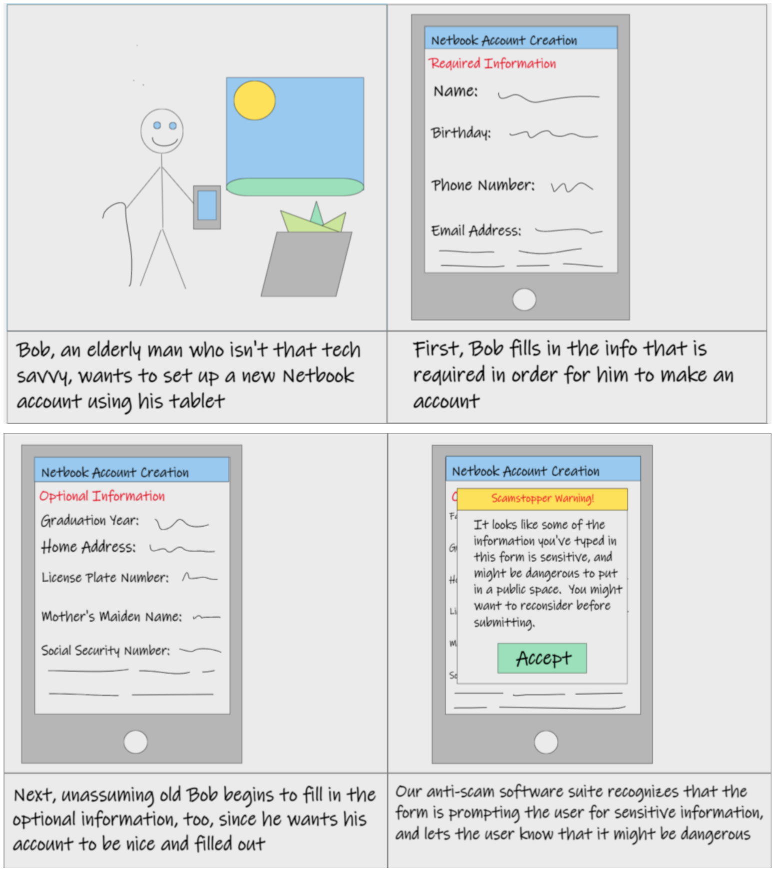
Figure 1 (Scenario 1):


Before
The IRS keeps emailing me to pay them with Subway gift cards
That sounds like a scam.
Are you saying I'm too dumb to tell if it's a scam?
Not at all! Scams affect everyone! This software helps me.
I guess I'll give it a try.
After
what's this? More gift cards?
Inbox
IRS
School
Wow! It is a scam!
Inbox
Subject: Gift Cards
IRS
*Warning This message looks like a scam
Block
Ignore
That was easy, and I just saved $500!

<u>Scenario 2:</u>

Bob is retired and a new owner of a tablet he bought in order to keep in touch with his children and grandchildren. He hasn't had any social media experience in the past and is still trying to understand technology in general. Bob searched online for social media apps and found Netbook, which he can't quite remember the exact name of but it sure sounds like the app that is on the news all the time. He begins making an account without realizing that the application is fraudulent and made only to get information from less tech savvy individuals. Since Bob has never signed up for a social network before, he didn't think much of the questions they asked since he believed this was all normal procedure for making any social media account. Questions start popping up on the form like "License Plate Number" and "Social Security Number" which the software recognizes as information that should not be entered for an untrusted source like Netbook and instantly warns Bob of the dangers this website has. Bob reads the warning message and realizes that the application he was trying to make an account with was a fake and does not enter anything else into the account creation form. This saves Bob's private information and keeps his trust in using the internet knowing that our software runs in the background to help prevent him from leaking any private data in the future.

Figure 2 (Scenario 2):



Bob, an elderly man who isn't that tech savvy, wants to set up a new Netbook account using his tablet

First, Bob fills in the info that is required in order for him to make an account

Next, unassuming old Bob begins to fill in the optional information, too, since he wants his account to be nice and filled out

Our anti-scam software suite recognizes that the form is prompting the user for sensitive information, and lets the user know that it might be dangerous