Project Proposal: ScamWatch

Anmol Mazoo, Arshdeep Singh, Kassandra Montgomery, Molik Verma

February 12, 2024

Info 4190 S50

Table of Contents

1.0 Abstract/Summary

In this digital age, thousands of people are getting scammed online every day, costing victims millions of dollars and often destroying lives. For example, in 2022, the Canadian Anti-Fraud Centre received nearly 71,000 reports and estimate that only up to 10% of fraud victims submit a report. Of the reported victims, the total monetary amount lost was approximately $500 million (Royal Canadian Mounted Police, 2023). This does not account, however, for the emotional and mental trauma these scams inflict.

These scams and frauds often begin through interacting with phishing emails, malicious ads and websites, and responding to fake phone calls. Two of the most common scams include tech support scams and refund scams. In both scams, the first critical goal of the scammer is to have the victim download a remote connection software and connect to their computer. To do so, In the case of a refund scam, the scammer will often tell the victim that to provide the refund, they need to connect their computer to the scammer's "company's server" and fill out a refund form. From there, the scam may vary, however will result in having the victim send them money.

Regardless of the persuasion tactics and the details of the scam, once this connection has been made, the scammer has full control over the victim's computer and access to any stored private information. Furthermore, the connection details, such as ID and password, are stored and the connection can be re-established provided the target's computer is on and the software is running. Ultimately, this connection can result in identity fraud, bank account and other financial information access, ransomware attacks and installation of malicious software, extortion, and more.

While there are many people who can identify and avoid falling for these scams, there are many people who are unable to. These people may be older, have medical or health issues, are financially struggling, or are simply inexperienced or uneducated in cybersecurity and digital technology. These people can very easily be lured into these scams and be taken advantage of.

As this is evidently a very serious issue and one that will continue to be one, we hope to create a software, called ScamWatch, which will be aimed at providing protection for individuals against remote connection scams. This software, designed to run discreetly in the background, will serve as a proactive defense mechanism by blocking unauthorized remote-control access and installations of common remote-control access (RCA) applications such as AnyDesk and TeamViewer. If an RCA application is already installed, users will receive alerts for any connection attempts, signaling potential scams. Of course, there are legitimate uses for RCA applications. Due to this, users will be able to temporarily disable the software's blocking function for the expected use. Finally, ScamWatch will additionally offer educational content on common scam tactics, empowering users to stay vigilant.

2.0 Aim

The main aim of this project is to develop a software that helps provide an extra layer of protection against remote connection scams.

3.0 Objectives

The following objectives outline how we intend to successfully complete this project:

- Research and analyze remote connection scam tactics targeting people.
- Learn more about password protection and multi-layer authentication methods.
- Determine which resources and tools are necessary for the software development.
- Explore more on determine how to prevent the execution of certain applications.
- Investigate on way to stop the third party from disabling the anti-scam application
- Develop mechanism to alert the person if a suspicious connection is made.
- Design user-friendly interface prioritizing ease of use for older users.
- Design different types of tests for different scenarios

4.0 Project Schedule

The following schedule shows a breakdown of the project including time for research, planning, development, and testing. It additionally shows dependencies as well as deliverables throughout the project.

	Task Name	Duration	Start	Finish	Predecessors	Notes
1						
2	**1 ScamWatch Application**	**125 days?**	**Mon 24-02-12**	**Mon 24-07-29**		**Deliverables:**
3	**1.1 Plan & Research**	**15 days?**	**Mon 24-02-12**	**Fri 24-03-01**		
4	1.1.1 Functional & Non-Functional Requirements	11 days?	Mon 24-02-12	Mon 24-02-26		Deliverables: Functions Report
5	1.1.2. Analyze RCA Related Scams & Determine Use Cases	11 days?	Mon 24-02-12	Mon 24-02-26		Deliverables: Use Case Diagram(s)
6	1.1.3 Determine requirements	11 days?	Mon 24-02-12	Mon 24-02-26		Deliverables: Requirements Outline
7	1.1.4 Compile Resources	15 days?	Mon 24-02-12	Fri 24-03-01		
8	**1.2 Implementation**	**88 days?**	**Mon 24-03-04**	**Thu 24-06-27**	**3**	
9	**1.2.1 Function 1: RCA Application Blocker**	**19 days?**	**Mon 24-03-04**	**Mon 24-03-25**		Deliverables: Working function
10	1.2.1.1 Research Application Blocking Methods	5 days	Mon 24-03-04	Fri 24-03-08		
11	1.2.1.2 Design Logic	3 days?	Sat 24-03-09	Tue 24-03-12	10	
12	1.2.1.3 Code Function	8 days?	Wed 24-03-13	Fri 24-03-22	11	
13	1.2.1.4 Test Function	3 days?	Sat 24-03-23	Mon 24-03-25	12	
14	**1.2.2 Function 2: Connection Alert**	**61 days?**	**Mon 24-03-04**	Tue 24-05-21		Deliverables: Working function
15	1.2.2.1 Research Connection Alerting Methods	4 days	Wed 24-03-27	Sat 24-03-30		
16	1.2.2.2 Design Logic	5 days?	Mon 24-04-01	Fri 24-04-05	15	
17	1.2.2.3 Code Function	26 days?	Mon 24-04-08	Mon 24-05-13	16	Note: Semester Break Falls Here
18	1.2.2.4 Test Function	6 days?	Tue 24-05-14	Tue 24-05-21	17	
19	**1.2.3 Function 3: Knowledgebase**	**17 days?**	**Wed 24-05-22**	**Thu 24-06-13**		Deliverables: Working function
20	1.2.3.1 Write & Compile Helpful Information, Advice, & Links	8 days?	Wed 24-05-22	Fri 24-05-31		
21	1.2.3.2 Code Function	5 days?	Mon 24-06-03	Sat 24-06-08	20	
22	1.2.3.3 Test Function	4 days?	Mon 24-06-10	Thu 24-06-13	21	
23	**1.2.4 Develop UI**	**10 days?**	**Fri 24-06-14**	**Thu 24-06-27**	**9,14,19**	Deliverables: Working UI
24	1.2.4.1 Design UI	2 days?	Fri 24-06-14	Mon 24-06-17		
25	1.2.4.2 Code UI	4 days?	Tue 24-06-18	Sat 24-06-22	24	
26	1.2.4.3 Test UI	4 days?	Mon 24-06-24	Thu 24-06-27	25	
27	**1.3 Prototype**	**19 days?**	**Wed 24-07-03**	**Mon 24-07-29**	**8**	Deliverables: Final Product
28	1.3.1 Final Research	1 day?	Wed 24-07-03	Wed 24-07-03		
29	1.3.2 Final Refinements	12 days?	Thu 24-07-04	Fri 24-07-19	28	
30	1.3.3 Final Testing	6 days?	Mon 24-07-22	Mon 24-07-29	29	

5.0 References

Royal Canadian Mounted Police. (2023, February 27). Fraud Prevention Month 2023: *Fraud losses in Canada reach another historic level*. Royal Canadian Mounted Police. https://www.rcmp-grc.gc.ca/en/news/2023/fraud-prevention-month-2023-fraud-losses-canada-reach-historic-level