



Private protector

SECURITY. PRIVACY. LOYALTY.

Proficiência Pessoal e Interpessoal

3.º ano / Turma 3 - MIEIC 2020/2021

Teacher: Fernanda Teixeira Torres

Group members:

Ana Inês Oliveira de Barros

up201806593@edu.fe.up.pt

Bernardo António Magalhães Ferreira

up201806581@edu.fe.up.pt

Eduardo da Costa Correia

up201806433@edu.fe.up.pt

João Alexandre Lobo Cardoso

up201806531@edu.fe.up.pt

João de Jesus Costa

up201806560@edu.fe.up.pt

João Lucas Silva Martins

up201806436@edu.fe.up.pt

Table of contents

Table of contents	2
Introduction	3
Initial proposal	4
Motivation	4
Relevance	4
Features	6
Subscription Plan	6
Budget breakdown	7
Return on investment (ROI)	8
Market Study	9
Competitor analysis	9
SWOT analysis	10
PEST analysis	11
Product Requirements	11
Implementation stages	13
Product technical features	14
Jurisdiction	14
Technology	15
Privacy	15
Security	16
Trust and marketing	17
Design	17
Conclusion	18
Glossary	19
Bibliography	20
Technical sheet	21
Task Distribution	21
Critical analysis of the group	22
Annex	24
Annex A - Questionnaire Results	24
Annex B - Mockups	26
Info	28

Introduction

This report aims to describe our proposal for an innovative project for the faculty course of PPIN. The proposed project in question is *Private protector*.

Private Protector is a web platform whose main goal is to make the online life of our users secure and private without impacting their convenience. The platform will include several services with different purposes, such as: an email service with end-to-end encryption, a utility to reserve usernames, and a service that notifies about security flaws and leaks that may be affecting the user. The transition to using our platform is as simple and straightforward as creating a new email account and will be aided by multiple tips and guides to improve the user's online privacy.

Since our objective is to provide a service in which our users can rely on and place their loyalty, our product will have a free tier, so anyone in the world can use our platform and get the basics needed to protect their rights, regardless of their financial capacity.

“[...] But saying that you don't need or want privacy because you have nothing to hide is to assume that no one should have, or could have, to hide anything -- including their immigration status, unemployment history, financial history, and health records. You're assuming that no one, including yourself, might object to revealing to anyone information about their religious beliefs, political affiliations, and sexual activities, as casually as some choose to reveal their movie and music tastes and reading preferences.” (Edward Snowden in Permanent Record, September 17, 2019: 176).

Initial proposal

Motivation

Our work is motivated by the state of the current privacy focused market, which is highly fragmented and still does not provide a solution for the people's needs. Given recent world events, an increasing number of people are worrying about their online security and privacy without a convenient and trustworthy platform, with the services they need, to turn to.

According to the *Have I Been Pwned* tool which collects and analyzes hundreds of database dumps, in the first 4 months of this year (2021), 600 million accounts have already been compromised. Along with compromised accounts, data leaks have become a frequent phenomenon and security standards, both from business and the government, are kept low. These are all problems that need to be solved. However, our biggest motivation is the right to privacy, the 12th article stated in the Universal Declaration of Human Rights which continues to be neglected by society.

We believe that the damages caused by problems such as: data leaks, difficulty in maintaining a safe online identity, and the lack of transparency about the current threats to security/privacy, can be mitigated by better security practices and a real investment in development and design. We want to grab this opportunity to provide a tool that helps users protect themselves against these dangers online.

Relevance

Even though some recent measures and regulations (such as the GDPR in Europe) attempted to tackle these user privacy and safety issues, we believe that these steps are not enough, as they are not effective at deterring big companies.

Nowadays, it is undeniable that social media plays a huge part of our society. For most people, many of their daily social interactions are made through social networks, and the ongoing COVID-19 pandemic accentuated this trend. As such, companies that own social media websites have access to the personal information of millions of people. This includes large amounts of potentially sensitive information,

i.e., a person's daily routine, personal preferences, location, phone call history, friends and family information, and much more.

Millions of records are still being stored and later processed by a plethora of increasingly robust and privacy-threatening algorithms. This recent development is a double-edged sword. On the one hand, data mining is proving to be an amazing tool to infer decisions and trends within complex models. On the other hand, given that most data collection does not go through anonymization processes, it becomes a hazard to individual privacy. There is a need for protection from these unlawful and unethical practices, so data mining and data collection can be done ethically.

“The primary reason for curtains/blinds/drapes covering our windows in our house is to stop people from being able to see in. The reason we don’t want them to see it is because we consider much of what we do inside our homes to be private. Whether that be having dinner at the table, watching a movie with your kids, or even engaging in intimate or sexual acts with your partner. None of these things are illegal by any means but even knowing this, we still keep the curtains and blinds on our windows. We clearly have this strong desire for privacy when it comes to our personal life and the public.” (Joshua in The Crypto Paper).

For example, facial recognition Artificial Intelligence algorithms are used in China and the United Kingdom (among others) not only to “crack down in crime and terrorism”, but also to spy on the citizens and “to silence political foes, track dissidents, and round up ethnic minorities in regions such as Xinjiang”. [3]

A more relevant example to the reader may be Facebook's data breach, in which the personal information of 533 million users was leaked and shared online, “[...] including phone numbers, email addresses, birthdays, and other personal details [...]” [4].

In the internet age, privacy has become a difficult thing to maintain. Our app intends to help users protect their data. We currently do not have the means to prevent these tremendous misuses of personal information, but we can help with minimizing your data collection and ensuring a more private internet browsing experience.

Features

Since our aim is to help users protect their privacy online, our application gathers features that provide security.

The first and main feature of our product is a **private and secure email service**. It shall use secure technology to protect the user's information (see *Product technical features* section, *Security* subsection). Along with the email service, we want to help users protect their information. To achieve this, we will gather a **notification system** that notifies users whenever their personal information is found online. Also, we plan on providing easy access to **tutorials and guides about privacy**, to help educate our users on the subject. Some extra features that will make it easier for the user to maintain a unique identity are **aliases** and **username reservation**. The former provides the user with the ability to compartmentalize their online activity, while the latter also informs the user about applications where their favorite username is available.

Along with these, our service will offer **upgradable storage, email forwarding**, and the ability to create **mailing lists**. Although it is difficult to implement correctly, we also plan to have anonymous **remote content loading** to increase the user's online privacy. **Integration with popular email clients** (like thunderbird) is also a must-have feature for our users. Not only does this attract users that wish for better privacy while keeping a familiar environment, but it also gives users some freedom regarding the tools they wish to use. For those users that prefer to try something new, we provide a **rich and responsive web interface**.

Subscription Plan

We will offer different plans with a monthly subscription with distinct, optional, subscription-based functionalities. With this structure, we provide a free option, so clients only need to upgrade their current plan if they find a need for extra storage and/or extra features. However, we plan on maintaining all premium plans free for non-profit organizations.

A paid subscription provides extra aliases and storage, automatic answers and mailing lists for the email service. An example of an unlockable premium functionality would be username reservation in applications.

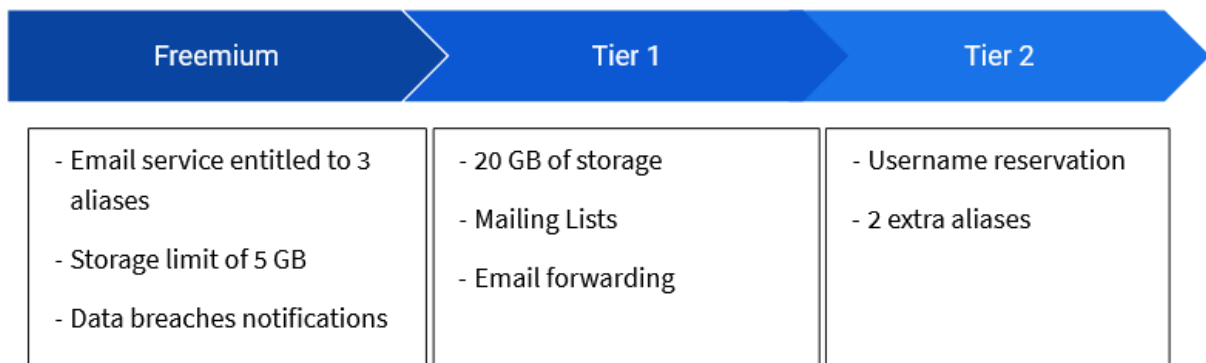


Fig 1: Upgradable plans example.

The premium features planned for the initial release of the application are as follows:

- **Aliases** - a user can acquire extra aliases (up from the 3 base).
- **Storage** - users can enhance their storage capacity.
- **Automatic email answering** - Email received that satisfies the pre-established conditions by the user, are automatically answered.
- **Mailing lists** - Users can create lists to communicate with teams easily.
- **Email forwarding** - Users can automatically forward their email to another address.
- **Custom domain** - Users can use their own domains for their email addresses.
- **Username reservation** - Automatic username reservation on multiple websites.

Budget breakdown

In order to achieve our business goals, we need to purchase private servers and to develop the web application. Both these requirements would have an initial investment and high cost maintenance. Along with these expenses, we plan on subscribing to a low-cost captcha solver that does not compromise our users' privacy. Taking all this into account, our estimated budget, in euros, is 50,000 for the complete project or 35,000 for the intermediate version.

5-10k	Servers	<ul style="list-style-type: none"> 1k - renting servers 9k - buy a personal server
20-35k	Web application	<ul style="list-style-type: none"> 10k - Prototype development ~25k - Final product development Ceiling of 35k for website maintenance
8k	Website design	<ul style="list-style-type: none"> 2k - Design 6k - Features and user stories implementation
1-2k	Captcha solvers	<ul style="list-style-type: none"> 500 - Initial contract Prediction of 2k to handle requests of premium users
30-60	Website's domain	<ul style="list-style-type: none"> An average of <u>30€</u> per year for the website domain
0,72k-1,8k	DDoS Protection	<ul style="list-style-type: none"> ~10€ - Basic DDoS protection in early stages Gradually invest in better protection along with community expansion

Fig 2: Expenses plan in euros

Return on investment (ROI)

As explained above, we estimate an investment of **50 thousand euros** for the complete project, which will take two years to achieve. We believe our premium users will pay, on average, a monthly subscription of **5 euros** for our product. In two years, a single premium user will spend **120 euros** on our product. This analysis aims to calculate the **return on investment** of our product according to the number of premium users we gather in **two years**. To calculate the return on investment, we follow the following formula:

$$ROI(\%) = \frac{Benefits - Costs}{Costs} \times 100$$

To achieve a **breakeven** state, since a single user spends 120 euros in two years, we need at least **416 users** to pay for a premium subscription during this time frame. In other words, this is equivalent to a ROI value of 0%. To achieve a higher value, we need more than 416 users to pay for a premium service. Duplicating the number of premium users gives us a benefit of 96 thousand euros, which results in **92% ROI** value. Settling for 1000 premium users benefits 70 thousand euros and results in a **40%** profit value.

This ROI analysis is simplified, because it assumes that premium users pay an average of 5 euros per month consistently for the two-year time frame. However, this value can change and may vary from user to user due to discounts and other

factors. Also, these calculations take for granted that the investment will be of 50 thousand euros, but this cost was the result of an estimation which results in uncertain, but likely ROI values.

Market Study

Competitor analysis

Since online privacy is a common theme nowadays, there are a lot of apps currently available on the market focused on helping users protect themselves online. Listed below are the most popular services that we consider to be our competitors:

- [Have I Been Pwned](#) - Checks if your personal information has been compromised;
- [Earlyname](#) - Claim usernames early in web services;
- [Mailbox](#) - Secure email service aimed at companies;
- [Posteo](#) - Independent email service;
- [Disroot](#) - Application service suite against whistleblowers;
- [ProtonMail](#) - Free encrypted email service;
- [Tutanota](#) - Email service which invests on the research of new security focused technologies.
- [StartMail](#) - A private e-mail service.

Although some of these companies provide their services free of charge, the majority of them have both options: free and paid service. The paid service, often referred to as 'premium service', is a version of the product with extra functionalities and/or fewer restrictions on usage. The paid service has an average price of \$20 per month.

Most of these companies provide features that we desire to provide to our customers. However, none of them gather all of these features in one product. Currently, if a person wishes to take advantage of all these features, they would have to buy/use multiple products, which might only have some features they are

interested in. This means that many of our competitors have a high entry barrier that we wish to mitigate in our product.

Another point we took into account is that none of these apps are perfect. Every product mentioned contains at least one defect, most common being forcing the user to use their app/missing integrations with third-party apps like Thunderbird, only supporting non-private payment methods, like PayPal, or being based in a country belonging to the 14 eyes.

Our aim is to fill this gap in the market by providing all of these services in one package, with a lower entry barrier as well numerous improvements.

SWOT analysis

Strengths

- Centralize related resources in an intuitive way.
- Focus on working on top of progress already made in the field by identifying and working on its failures.
- Appeal to a broader audience than the competition by providing advantages to the “everyday person” (not focusing on “power users”).
- Allows “power users” to collaborate on the project and integrate it in other platforms.
- Independent collaborative work allows us to ship features faster and to get preemptive approval from the users.

Weaknesses

- A lot of similar-looking projects are already in the market.
- Appeals to a limited market.
- Difficult to advertise.
- Broad scope.

Opportunities

- A lot of discussions are present in the media relating to privacy.
- Recent scandals related to data leaks and misuse.
- Much of the more online privacy-aware community expresses distaste for the currently available solutions.

Threats

- Pressure by hostile organizations and/or governments to cease

operations/disclose user information.

- Companies with more market presence can shadow our business.
- Our competition “hyper-focuses” on parts of our business.

PEST analysis

- **Political**
 - It is possible to make all data centers/server houses “green”, thus abiding by any environmental protection laws.
 - Although they are legal, many countries might act with hostility to our services, by trying to make them illegal.
- **Economic**
 - We have to maintain “technical debt” under control (especially in the early days).
 - Early investment in external security audits to gather consumer trust.
- **Social**
 - Can be framed as a product for criminals by bad actors.
 - Only appeals to the “tech-savvy” demographic.
 - Potential for advertisement by key figures in social media.
- **Technological**
 - Low barrier to entry.
 - Needs constant development of the platform (full-time developers).
 - Needs periodic audits.
 - Innovation is important to stay ahead of the competition.

Product Requirements

Due to the multipurpose nature of our product, we will need a substantial initial investment in order to ensure the basic functionalities of the service are available on the initial delivery. In this section, we specify these requirements.

The main focal point of our project is the web application, which will help us grow as a community and as a company. The best solution would be to purchase our own servers, but this is not initially possible, because of our small budget. As a

result, we are obligated to use **rented servers**, which we will replace in the project's future.

A **small team of developers** will be responsible for the development of our web application, our website and all of their planned features (as described previously). Since all of us have some experience in developing websites, this problem is likely already solved.

Security audits will be scheduled after each major release to assist us in finding and fixing different software vulnerabilities that may expose our services. If any of our users' data were to be leaked, the reputation of our company would be greatly compromised and our project would take a massive hit in popularity. Thus, it is vital to ensure that no vulnerabilities happen in the first place.

A **design team** will also be involved in designing and ensuring that our service features seamless and accessible interfaces. They will work hand in hand with our programming team to achieve this goal.

In order to provide automatic account creation for username reservation, we need to acquire an **automatic captcha solver** to bypass the captchas that appear during account creation. This is a mandatory step if we want to create accounts to reserve usernames for our users. Since this feature is not considered to be of high priority, the captcha renting will be postponed to the mid-end of the project.

As soon as our site has a stable viewership, we plan to invest in a **marketing team**, which will aid us in advertising our services. This will grow our community, help us increase awareness about privacy concerns and assist us in gathering the necessary investment to implement the remaining planned features.

To maintain a better relationship with our users, we are planning on hiring a **human resources team**, with the purpose of interacting and promoting events within the community. People are most likely to share and trust in companies which have a good image and reputation.

A latter investment would be acquiring **private servers**. The main driving factor behind this purchase is to help us become independent of third party servers, and, as a consequence, all user data and credentials will be stored in servers that we can fully trust. It will also host our website, used by our web app, replacing the servers rented during the initial steps of the project. This step is considered a priority, but, due to it being highly expensive, it will only be taken into account at a later stage of the project.

Implementation stages

One of the most common practices in the software industry is to write **user stories** to streamline the development process. This will help the team and the stakeholders grasp the main features of our application, preventing future misunderstandings.

“In software development and product management, a user story is an informal, natural language description of features of a software system. They are written from the perspective of an end user or user of a system, and may be recorded on index cards, Post-it notes, or digitally in project management software. Depending on the project, user stories may be written by different stakeholders like client, user, manager, or development team. [7]”

The next step would be to **convince stakeholders** and **gather investment** from privacy focused entities. To facilitate this goal, we plan on using and expanding on the work developed and experience we got from the PPIN class, i.e., this report and our presentation. This stage is vital to ensure that we can advance with our plan, so it will be our top priority in the early stages of our project.

When sufficient funding is acquired, we intend to **start the development** of our web service as soon as possible. To guarantee a short and long term success of the web app, the Django framework will be used for backend development, due to its security-focused features. For the frontend process, we are torn between using either Vue.js or React. With these web frameworks, the development of the application will be easier and faster.

We predict that our project will be completed within around 2.5 years, but we see the possibility of releasing an intermediate version as soon as 1.5 years into the development cycle. This prototype is estimated to be available by the first semester of the second year of development. However, before this can happen, our company needs to rent servers. Although this creates a dependence on other companies that provide these servers, at this point, we won't be able to afford the costs of acquiring and maintaining our own servers. That is a goal that we intend to achieve when we start making a profit.

With an intermediate version available, we can gather community feedback. This results in a phase fully focused on the product where our team will be

committed to fixing bugs and improving the service provided. This phase is also a good moment to reconsider some features and to introduce new ones. By the end of this stage, we want to make the freemium subscription available.

We believe that this next phase is the most important stage to invest in marketing. This is because we will have secured some users and ironed most of the *bugs* and problems present in our service, so we will be very attractive to new users. The influx of new users brought by well-placed and honest marketing campaigns has the power to promote our application further, thus securing the funds needed for the next implementation stage.

Eventually, when we acquire enough users buying premium plans, we will be financially able to transition from rented servers to self-hosting. We will opt for eco-friendly hosting with green servers to reduce the environmental impact. Along with financial profit and as a consequence of an investment in marketing, at this stage we will have established a reputation which we will take advantage of to build a partnership with other services. Our plan is to partner with companies with the same vision as our product in order to provide better features. For example, a partnership with *Have I Been Pwned* would enable interesting features regarding data leaks.

After the final stage of implementation referred above, we need to focus on the future of our application. The continual refining and expanding of our service with new features, such as a Google Forms alternative, could attract new users from other audiences. Furthermore, the continuous support of our users and development of new features and security measures will always be the main objective of our team.

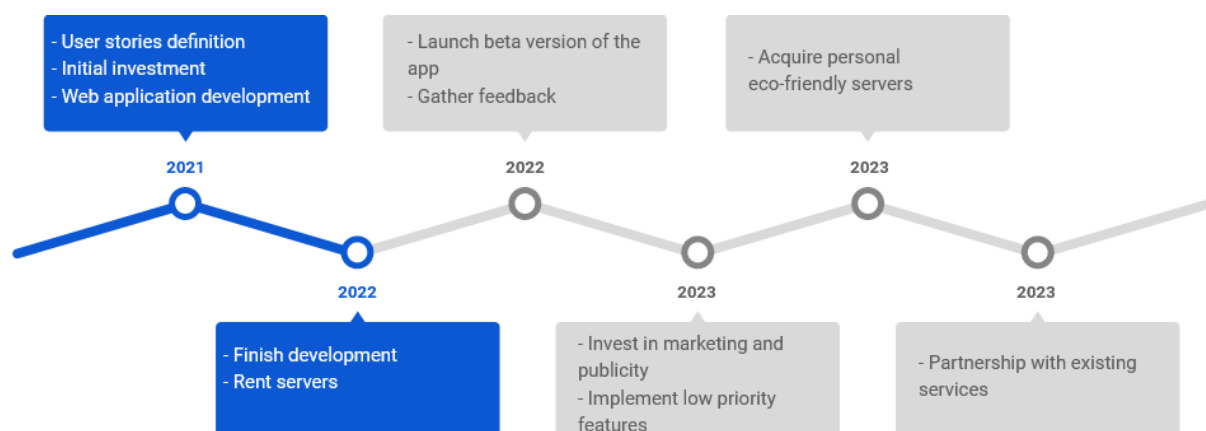


Fig 3: Business plan

Product technical features

Jurisdiction

We want our service to always operate outside the USA and the other **Fourteen Eyes** countries: Australia, Canada, New Zealand, United Kingdom, Denmark, Netherlands, France, Norway, Germany, Belgium, Spain, Sweden, and Italy. These fourteen countries' governments are known to spy on their citizens through mass surveillance and requiring backdoors on digital systems in their jurisdiction. This can prove difficult before we acquire our own servers, because most hosting companies do not offer services in Europe and North America outside these countries. This problem is mitigated by our **encryption at rest** policy.

We also have a preference for operating inside a country with strong consumer protection laws.

Technology

All account data will be encrypted at rest with zero-access encryption. All e-mail communication between users will be automatically and conveniently end-to-end encrypted (E2EE). Due to underlying technological limitations, this automatic encryption can only work between users of our service. Users that need to communicate with people not using our service should use **OpenPGP** (or similar) keys to ensure their communication is private. This will be eased by having support for **WKD**.

A **temporary mailbox** feature can also be added, so users can send encrypted emails without sending an actual copy of the contents to the recipient, should they be using a service without encryption at rest features.

Users will be allowed to use their own (custom) domain name. **Custom domain names** are important to users because it allows them to maintain their independence from the service in case of a problem/dissatisfaction. These custom domains should have **caught all** and/or **aliases** support.

In order to ensure customers can easily access, manage, and download their email, all these features' implementation should prioritize compatibility with standard

e-mail access protocols: **IMAP**, **SMTP** and/or **JMAP**. **Sub-addressing** support will also be prioritized to simplify working with aliases.

Privacy

Our application will take into account the protection of the user's information. In order to achieve this, we will block the sender's IP address from appearing in the header field and accept payments in the form of cryptocurrency or anonymous payment options. We will also have an onion service, so users can access the platform using the **Tor network**.

Personally identifiable information other than the user's username and password, which is necessary to login and register, will not be required. It is also important to mention that our service meets the requirements defined by the General Data Protection Regulation (GDPR).

Security

Since security is one of our main goals, our product takes into account a lot of measures and features regarding this topic. There are two sides to security in our application: keeping the information on our end secure, and providing features to help keep our users' accounts safe.

Firstly, to protect the contents of the servers in case of unlawful seizure (zero access encryption), we will implement encryption at rest (e.g., dm-crypt). Along with this, we plan to prevent the manipulation of data and forged domains with the help of **DNSSEC**, which is an extension improving the safety of the **DNS** protocol.

Secondly, we need to be aware that gaining unauthorized access to a user's account is the most obvious possible point of failure in our service. To work around this, account protection features like **2FA** and **hardware key authentication** will be implemented.

Lastly, the security of our platform should be evaluated by external entities, so we can be sure of its safety. We will hire an auditing company to validate the security of our services after every major release. We will complement this with **bug-bounty programs** and **coordinated vulnerability-disclosure** processes, thus discovering

vulnerabilities in our implementation ahead of time and allowing us to fix them in a timely manner. Furthermore, we aim to achieve the following:

- No TLS (1.2 or later) errors/vulnerabilities of any kind when profiling using testssl.sh.
- A valid MTA-STS and TLS-RPT policy.
- Valid DANE records with DNS CAA Resource Record.
- Valid SPF, DKIM and DMARC with the **policy p value** set quarantine.
- SMTPS submission (assuming SMTP is used).
- HTTP Strict Transport Security (HSTS).
- Subresource Integrity.
- Implementation of Authenticated Received Chain (ARC) (useful for users who post to mailing lists RFC8617).
- CSP
- Expect-CT

Trust and marketing

Maintaining the users trust is important for our company. For that reason, we will keep a public-facing leadership/ownership and frequent transparency reports, which will help build a relationship of trust between our company and the users of our service.

It is common for people to start distrusting marketing, given all the scandals, inconveniences, and problems it tends to bring. We believe that marketing can be done right, so we will *self-host* our analytics and comply with DNT requests. It is also important to not make irresponsible marketing claims, such as:

- “unbreakable encryption” (encryption can be broken in the future when technologies allow for it);
- “100% anonymity” (users can easily de-anonymize themselves);
- “100% secure” (we need frequent security analysis to ensure the security of the service).

The marketing team can also benefit from easy to read documentation, terms of service (inspire trust), and usage guides, for example, setting up 2FA and OpenPGP.

Design

Any successful website needs proper and professional design. Given that we strive to provide straightforward features and accessibility to our website, it makes sense that we pick a design that is simple, clear and easy on the eye, but also eye-catching. In order to achieve a simple and intuitive navigation, our design team will start the design process by creating *user flows* which will provide us with a simulation of the users' interactions with the web application. Then, it is important to design *mockups* with properly structured pages that will help visitors find each user interface element easily.

For the final result, we want to achieve a good and spacious UI/UX design with good contrast between elements. Regarding efficiency, our website should be fast, responsive and light. More importantly, we want anyone to be able to access our website regardless of physical limitations/disabilities. This includes, but is not limited to: keyboard only controls for those with arthritis, and semantic HTML elements and aria standard conforming features for those with vision disabilities.

Conclusion

This project allowed us to better understand the process that goes behind the planning and development of a project, since its conception until its implementation. We had to learn how to organize ourselves as a team, learn how to talk to an audience online and develop our soft skills regarding communication. A product presentation meant keeping a confident attitude regarding the service we are trying to sell and maintaining our audience engaged and interested in our presentation. We got the opportunity to work on our flaws to improve them. This is important for our future, where we will definitely take advantage of our experiences and apply the knowledge we gathered from the development of this report and presentation.

Regarding the innovative project, we believe that we tackled an important issue with modern technology and its misuse in our society. This meant that we also benefited from studying the issues at hand.

In the future, we would like to actually implement the ideas explored in this report as an actual project, since it fits in with our areas of interest and is something that we believe has a lot of potential. There's work developed for this course (PPIN) that could be reused for this possible future implementation of ***Private Protector***.

Glossary

- **CAA** - Certification Authority Authorization
- **2FA** - Two-factor Authentication
- **CSP** - Content Security Policy -
<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>
- **Expect-CT** - Expect Certificate Transparency -
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect-CT>
- **GDPR** - General Data Protection Regulation
- **IMAP** - Internet Message Access Protocol
- **POP3** - Post Office Protocol
- **DNSSEC** - Domain Name System Security Extensions
- **DNS** - Domain Name System
- **DNT** - Do Not Track
- **SMTP** - Simple Mail Transfer Protocol
- **DDoS** - Distributed Denial of Service Attack
- **WKD** - Web Key Directory

Bibliography

1. Snowden, Edward. 2019. *Permanent Record*. United States: Metropolitan Books.
2. Joshua. 2020. "The Crypto Paper". <https://github.com/cryptoseb/cryptopaper>
3. Lindsey, Nicole. 2019. "China's Privacy Challenges with AI and Mobile Apps". <https://www.cpomagazine.com/data-privacy/chinas-privacy-challenges-with-ai-and-mobile-apps>
4. Duffy, Clare. 2021. "Facebook will not notify the 533 million users exposed in online database". <https://edition.cnn.com/2021/04/09/tech/facebook-hack-user-notification/index.html>
5. Rivera, Maricel. 2021. "7 Steps to Writing the Perfect Project Proposal". <https://www.fool.com/the-blueprint/project-proposal>
6. Farooq, Umar. 2021. "Project Proposal". <https://www.businessstudynotes.com/finance/project-management/project-proposal>
7. Wikipedia. 2021. "User Stories" https://en.wikipedia.org/w/index.php?title=User_story&oldid=1021145927
8. ROI Formula, Calculation, and Examples of Return on Investment <https://corporatefinanceinstitute.com/resources/knowledge/finance/return-on-investment-roi-formula/>
9. Wikipedia. 2021. "Market research". https://en.wikipedia.org/wiki/Market_research
10. Nick Babich. 2020. "Web Page Design: A Comprehensive Guide". <https://xd.adobe.com/ideas/principles/web-design/web-page-design/>
11. DataGuidance. 2021. "Portugal: CNPD orders INE to suspend Census 2021 data flows to USA". <https://www.dataguidance.com/news/portugal-cnpd-orders-ine-suspend-census-2021-data-flows>
12. EU. 2021. "Does the GDPR apply to companies outside of the EU?". <https://gdpr.eu/companies-outside-of-europe/>

Technical sheet

Task Distribution

1. Ana Inês Oliveira de Barros - up201806593 (burro)
 - Introduction
 - Initial Proposal
 - Competitor Analysis
 - Implementation Stages
 - Product technical features
 - Conclusion
 - Glossary
 - Questionnaire
 - Mockups
2. Bernardo António Magalhães Ferreira - up201806581
 - Introduction
 - PowerPoint
 - Mockups
 - Market Study
 - Product Requirements
 - Implementation Stages
3. Eduardo da Costa Correia - up201806433
 - Introduction
 - Initial Proposal
 - SWOT Analysis
 - PEST Analysis
 - Slide presentation
 - Conclusion
 - Questionnaire
4. João Alexandre Lobo Cardoso - up201806531
 - Product Requirements
 - Initial Proposal
 - Mockups
 - Questionnaire

- Implementation Stages
- Market Study
- PowerPoint

5. João de Jesus Costa - up201806560

- Introduction
- Initial Proposal - Motivation
- Features
- Market Study
- Competitor analysis and research
- Product technical Features
- Conclusion
- Bibliography
- Icon
- Slide presentation

6. João Lucas Silva Martins - up201806436

- Slide presentation
- Initial Proposal
- Requirements
- Implementation stages
- Product technical features
- Glossary
- Introduction
- Conclusion

Critical analysis of the group

During the development of this report, we were faced with a challenge: teamwork with more team members than we were used to. For this reason, we focused on the group's communication throughout the development of this report. To do this, we made sure to have weekly meetings. During these meetings, we would update each other on the work progress and redefine task assignments. Each week, we would update our to-do list and assign tasks to each member of the group, which resulted in a smooth development of the project.

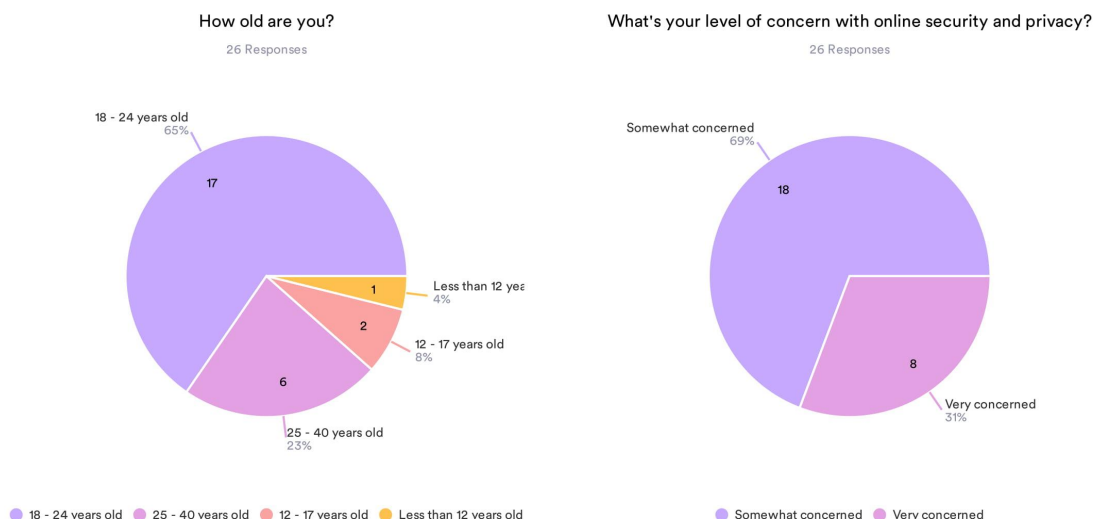
Regarding the conception of the product, we tried to maintain a pleasant team environment, which contributed to higher creativity and great exchange of ideas. Important decisions were made as a group.

Overall, our group chemistry worked well, and we believe that this shows in the quality of the work developed.

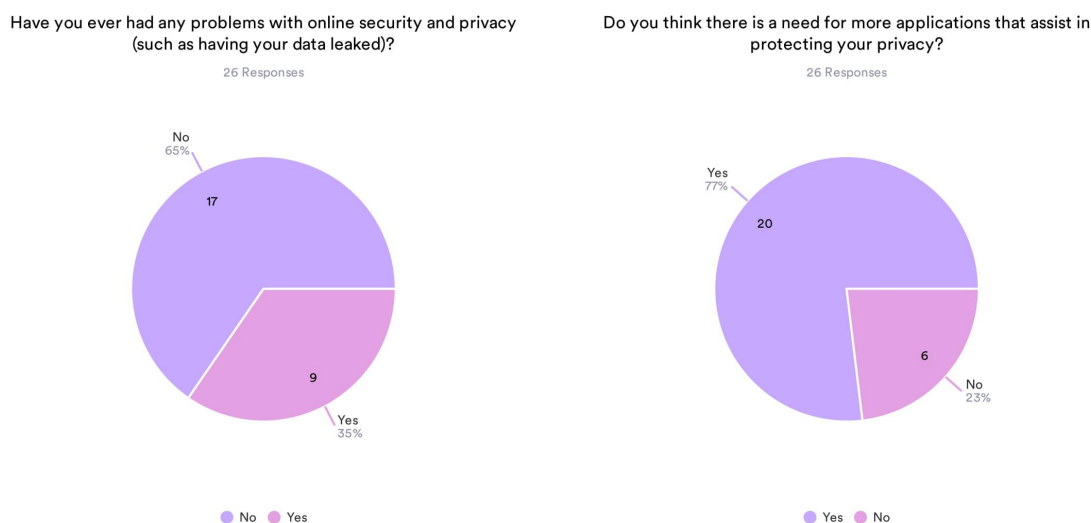
Annex

Annex A - Questionnaire Results

Relevance of a privacy focused web application



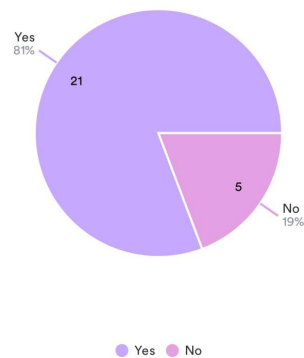
Relevance of a privacy focused web application



Relevance of a privacy focused web application

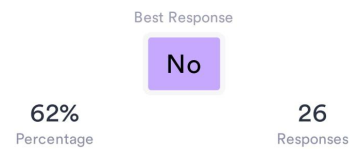
Would you be interested in a web service that provided ways to protect yourself on the internet, such as a private e-mail service and information about data leaks?

26 Responses



Would you be interested in a username reservation feature? (Accounts with your username would be created for you when available)

26 Responses

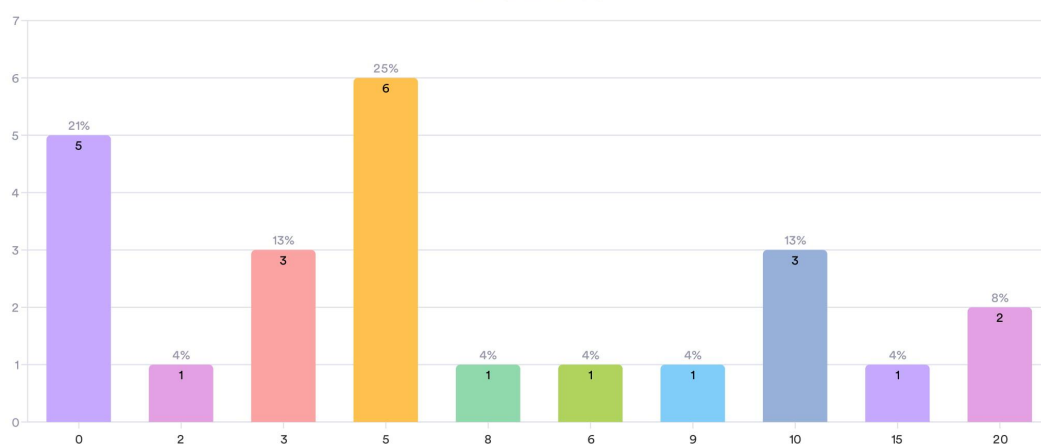


Data	Response	%
No	16	62%
Yes	10	38%

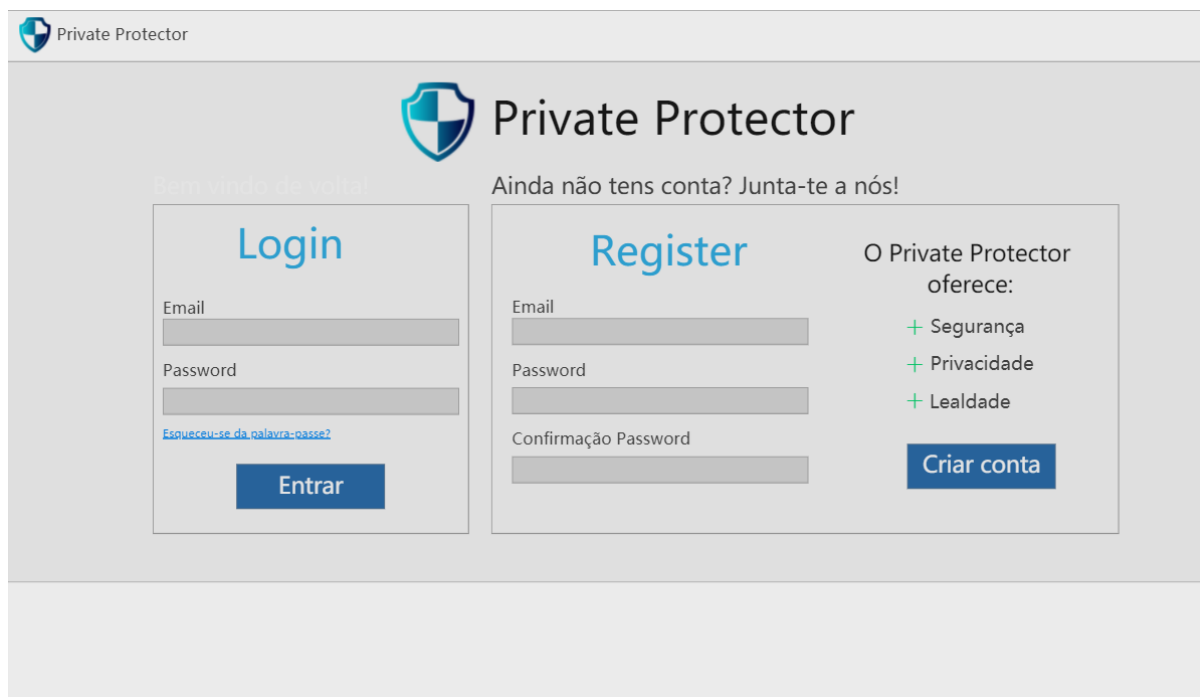
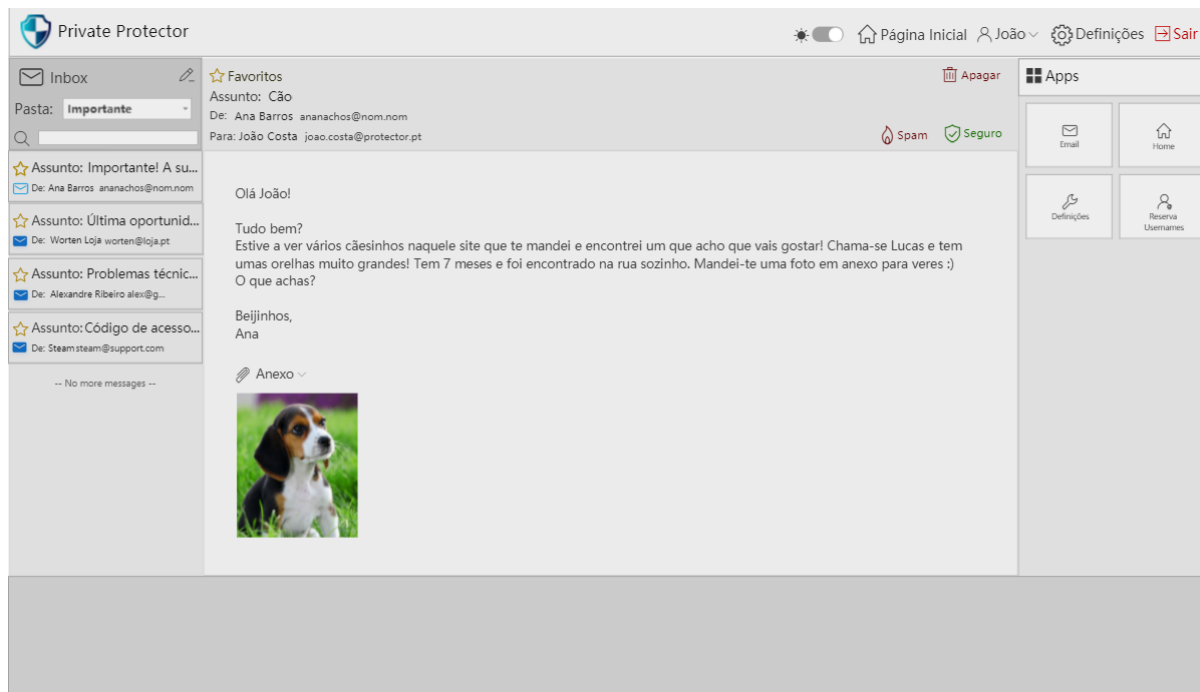
Relevance of a privacy focused web application

How much would you be willing to pay monthly for a premium service with extra services? (\$)

24 Responses- 2 Empty



Annex B - Mockups






Private Protector


Novos Vazamentos | Notícias | Verificar Vazamentos

Procura email / telemovel...

Encontrado em 2 vazamentos de informação!

	Facebook 12/05/2021 Ver mais	500 Milhões
	Twitter 13/03/2021 Ver mais	300 Milhões










 Aprende como te podes proteger:
 Guia: <https://www.protegete.com>

 Segue estes passos para protegeres as tuas contas:
 Guia: <https://www.protegete.com>

Private Protector

Novos Leaks | Notícias | Pesquisar Leaks

Os Leaks mais recentes:

	Facebook 12/05/2021 Ver mais	500 Milhões		Twitter 13/03/2021 Ver mais	300 Milhões		Discord 15/02/2021 Ver mais	50 Milhões
	LinkedIn 12/12/2020 Ver mais	250 Milhões		Livpure 1/11/2020 Ver mais	100 Mil		Tinder 09/09/2020 Ver mais	85 Milhões
	ParkMb. 8/05/2020 Ver mais	20 Milhões		Tumblr 3/02/2020 Ver mais	15 Milhões		MySpace 24/05/2018 Ver mais	2 Mil