A Spamless Internet

Viruthagiri Thirumavalavan

February 2019

Contents

About Us

Company Name	Dombox, Inc.
Primary Business	Webmail Service
Problem Solved	Email Spam & Internet Privacy
Author	Viruthagiri Thirumavalavan
Official Contact	giri@dombox.org
Company Website	www.dombox.org

Proprietary Notice

Fair Use Notice

Vision Statement

> A Spamless Internet

As of 2018, 3.8 billion[1] people use email in the world. That's more than half of the world population. We want every one of them to be spam free in the future.

Mission Statement

> A Spam Less Internet

We need a milestone that can be achieved in the near future.

Our mission statement says that we want less spam on the Internet. So we want at least 1 billion people to be spam free in the next 10 years.

Competitors

> Gmail, Outlook, YahooMail

Note: Users can use our product without switching their old mail account. Meaning... they can have @gmail.com address but still can use our mail service with the help of **mail forwarding**.

Product Tagline

> **The Zero Spam Mail Service**

Our proposed new system doesn't have the "Spam" folder.

[1] https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf

Chapter 1: Problem Analysis

Problem Summary

Email Spam is what's known as **Tragedy of the Commons**[2]. i.e. Spam email degrades the usefulness of the email system and increases the cost for all users of the Internet while providing a benefit to only a tiny number of individuals.

First spam mail was sent in 1978[3]. So it's a 40 years[4] old problem that's not solved yet. 281 Billion[5] Emails are being sent every day. That's around 102 Trillion emails in a year. 60%[6] of them are spam as of 2017. So almost 60 Trillion **spam emails** are being transmitted every year.

A 2009 research says spam costs 130 Billion[7] USD to the economy.

Around 40 countries[8] wasting their money on enforcing spam laws.

Email Spam can be termed as "Electronic Cancer". It's very hard to solve. Many innocent souls still being a victim of spam emails. e.g. Phishing, Malware, Scamming (Lottery scam[9], Employment scam[10], Nigerian scam[11], Romance scam[12] etc.).

Spam also started to play important role in Politics. e.g Fake News, Hilary Clinton email leaks[13] etc.

[2] https://en.wikipedia.org/wiki/Tragedy_of_the_commons
[3] https://www.templetons.com/brad/spamreact.html
[4] https://www.forbes.com/sites/courtstroud/2018/04/16/on-spams-40th-birthday-25-things-you-didnt-know-about-junk-email/
[5] https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf
[6] https://dev.to/matchilling/comparison-of-machine-learning-techniques-in-email-spam-detection--2p0h
[7] https://web.archive.org/web/20100317042916/http://www.ferris.com/research-library/industry-statistics/
[8] https://en.wikipedia.org/wiki/Email_spam_legislation_by_country
[9] https://en.wikipedia.org/wiki/Lottery_scam
[10] https://en.wikipedia.org/wiki/Advance-fee_scam#Employment_scams
[11] https://en.wikipedia.org/wiki/Advance-fee_scam
[12] https://en.wikipedia.org/wiki/Romance_scam
[13] https://en.wikipedia.org/wiki/Hillary_Clinton_email_controversy

Thus, there is a need for 100% foolproof spam detection and prevention system.

Our solution is not about fighting email spam. It's about killing email spam completely in the long run.

Introduction

Thousands of people tried to solve this problem. Even well-known people like Bill Gates tried to solve[14] it. But we settled for spam filters.

Spam filters are only **silencing** the spam problem, not **solving** it.

To quote Chris Hoffman from How-To Geek[15]

> Rather than solving spam, we've been forced to develop better spam filters to block it. If you use a service like Gmail, Outlook.com, or Yahoo! Mail, you have much better spam filters than you did a decade ago. It's impossible to fix spam without changing the way email works, so the problem will never be completely solved.

Although Chris has a point, we beg to differ

The problem is with the "Players". Not the "Game"

Trying to change the way email works is more like trying to change the way the postal system works just because some people abuse the postal system

Email system was not created for the modern internet. It was created way before the "world wide web" even existed and it does its job really well. i.e. Sending a message from one end to another.

In our system, we are not trying to change the "Game", but trying to set "Rules" for the "Players".

[14] https://www.theregister.co.uk/2004/01/26/well_kill_spam_in_two/
[15] https://www.howtogeek.com/180604/htg-explains-why-is-spam-still-a-problem/

Spam Statistics

281 Billion - That's how many emails sent per day in 2018, according to the research firm Radicati[16]

97% - That's the percent of spam emails sent in 2009, according to a Microsoft Security Report[17]

60% - That's the percent of spam emails sent in 2017, according to the website statista.com[18]

Since statista.com stat is recent, let's go with that number

If you do the math, the total amount of spam sent every year is ~ **60 TRILLION**

That's a crazy number.

The whole internet bandwidth is overloaded with spam traffic

Spam Filters

Keyword-based - Mails that contain words like "Viagra", "Nigerian King", "Penis Enlargement" etc most likely gonna get classified as Spam.

False Positives - If a genuine message contains spam keywords, there is a higher chance that the spam filter might classify that message as spam => Collateral Damage

False Negatives - When spam emails are marked as Genuine mails => Annoying

Not Bullet Proof - Experienced spammers know how to bypass the spam filters. If a spammer can figure out the spam algorithm/technique, then the spammer can able to bypass the spam filter by tricking the system.

Not Future Proof - What's preventing an experienced spammer from training an AI to bypass spam filters in the future?

[16] https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf
[17] https://blogs.msdn.microsoft.com/tzink/2009/04/09/97-of-emails-are-spam-says-microsoft-sir/
[18] https://www.statista.com/statistics/420391/spam-email-traffic-share/

Spam Damages

Productivity - No amount of money can give you back the time you lost. When computers get affected by malware emails, it would take many days (even weeks) to clean up the mess.

Scamming - Scammers target innocent people to scam them.

Network bandwidth - More than half of the Internet bandwidth is being wasted on carrying spam emails

Storage - Money is being wasted on storing spam emails

Spam Laws - Almost 40 countries are wasting their money on enforcing spam laws. Here is a nice article[19] that covers 28 countries spam laws

Political - Spam started to play important role in Politics. e.g Fake News, Hilary Clinton mails. (John Podesta account got hacked via a Phishing mail[20])

2009 research says[21], The estimate for the cost of spam mail in terms of lost productivity, energy costs and increased equipment cost is ~ **$130 BILLION** worldwide every year

How Spammers Get your Mail Address?

Leaked Databases - Account databases leaked by a hacker in public forums. This is their primary source.

Bad websites that sell your data for money - e.g. After you unsubscribe from their newsletters, your email address becomes useless to them. So they sell your data for some extra money

Good websites that have been a victim of hackers - e.g. Back in 2013, 150 million[22] Adobe accounts were hacked. Even recently Reddit[23] became a Victim of Hackers.

[19] https://blog.chamaileon.io/ultimate-email-spam-law-collection/
[20] https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/
[21] https://web.archive.org/web/20100317042916/http://www.ferris.com/research-library/industry-statistics/
[22] https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online
[23] https://www.wired.com/story/reddit-hacked-thanks-to-woefully-insecure-two-factor-setup/

Crawling - By crawling the web for the @ sign

Brute-force / Dictionary / Combinations - By trying multiple combinations of a name. For example, if your name is John Smith, the spammer might try the following addresses. john@gmail.com, smith@gmail.com, johnsmith@gmail.com, jsmith@gmail.com etc.

Why spam is still a tough nut to crack?

Internet-wide - For Facebook, spam is platform-wide problem. If you spam in Facebook, they can ban your account. But when it comes to email, the mail can be transferred from any internet domain and IP. So it's very hard to differentiate spammers from genuine senders. So email spam is an Internet-wide problem.

Design - You don't own google.com. But you can actually send emails from an address like @google.com. This is because the email protocol (SMTP) is designed exactly like our good old postal mail system. Mail can be handed over to multiple servers before reaching the recipient. So you can't ban a domain even if the spam emails are coming from that domain. You can ban only the spammer's IP address.

Cost - Sending spam emails literally costs nothing. Computing power is way cheaper now than before. So a spammer can rent a server for a few dollars and send out millions of spam emails. Domains also very cheap. So even if you ban a spammer's domain, the spammer may get another .com domain for $10

Lack of understanding - As the saying goes "To beat your enemy, you must know your enemy". While we can't expect an average internet user to know how a spammer operates, we must expect that from companies that fight spam. Gmail has 1.4 Billion[24] monthly active users as of 2018. There is no denying Gmail is an excellent mail service. However, they have a tiny flaw. But that tiny flaw has major consequences in fighting spam. [We can discuss this part later]

Botnets - Many naive users (Could be your Grandma) fall for the scammer's emails, install

[24] http://nymag.com/selectall/2018/04/how-to-turn-on-google-gmail-redesign-and-new-features.html

malicious software found in the email attachment and become part of a bot network (aka. Botnet[25]).

Botnets

Let us explain botnets in simple words.

When a computer becomes part of a botnet, it is called as “Bot”

The “Bot” act like a slave. It waits for the botmaster’s command and does that job. It can be anything. Sending spam emails to make money for the botmaster, Spread malicious attachment emails to more users and bring them to be part of the bot network, perform a DDoS attack, bitcoin mining etc.

Stopping the spammers in this case is very hard. You need to either remove the malicious software from all the slave computers found in the bot network or find the botmaster and put him/her in jail.

Banning IP address is not effective in the Botnet case. The botmaster got nothing to lose.

Simply put, any spam solution that’s not safe from BotNets is not really a spam solution at all.

Side note: Our system is safe from botnets

Top 10 Bot Networks

Based on the number of bots. i.e. Infected Computers

Name	Bot Count
BredoLab[26]	30,000,000
Mariposa[27]	12,000,000

[25] https://en.wikipedia.org/wiki/Botnet

Name	Bot Count
Conficker[28]	10,500,000+
Marina[29]	6,215,000
TDL4[30]	4,500,000
Zeus[31]	3,600,000
Ramnit[32]	3,000,000
Cutwail[33]	1,500,000
Akbot[34]	1,300,000
Sality[35]	1,000,000

Based on the Spamming Capacity

Name	Capacity
Marina[36]	92 Billion / Day
Cutwail[37]	74 Billion / Day
Srizbi[38]	60 Billion / Day
Grum[39]	39.9 Billion / Day
Rustock[40]	30 Billion / Day

[26] https://en.wikipedia.org/wiki/BredoLab_botnet
[27] https://en.wikipedia.org/wiki/Mariposa_botnet
[28] https://en.wikipedia.org/wiki/Conficker
[29] https://nulltx.com/top-4-largest-botnets-to-date/
[30] https://en.wikipedia.org/wiki/TDL4_botnet
[31] https://en.wikipedia.org/wiki/Zeus_(Trojan_horse)
[32] https://en.wikipedia.org/wiki/Ramnit
[33] https://en.wikipedia.org/wiki/Cutwail_botnet
[34] https://en.wikipedia.org/wiki/Akbot
[35] https://en.wikipedia.org/wiki/Sality

Name	Capacity
Conficker[41]	10 Billion / Day
Mega-D[42]	10 Billion / Day
Kraken[43]	9 Billion / Day
Bagle[44]	5.7 Billion / Day
Nucrypt[45]	5 Billion / Day

The Gmail Flaw

Gmail has a very good spam filter. But that doesn't mean Gmail don't have any flaws. Gmail has a minor but a critical flaw when it comes to spam prevention.

[36] https://nulltx.com/top-4-largest-botnets-to-date/
[37] https://en.wikipedia.org/wiki/Cutwail_botnet
[38] https://en.wikipedia.org/wiki/Srizbi_botnet
[39] https://en.wikipedia.org/wiki/Grum_botnet
[40] https://en.wikipedia.org/wiki/Rustock_botnet
[41] https://en.wikipedia.org/wiki/Conficker
[42] https://en.wikipedia.org/wiki/Mega-D_botnet
[43] https://en.wikipedia.org/wiki/Kraken_botnet
[44] https://en.wikipedia.org/wiki/Bagle_botnet
[45] https://www.computerworld.com/article/2536378/security0/top-botnets-control-1m-hijacked-computers.html

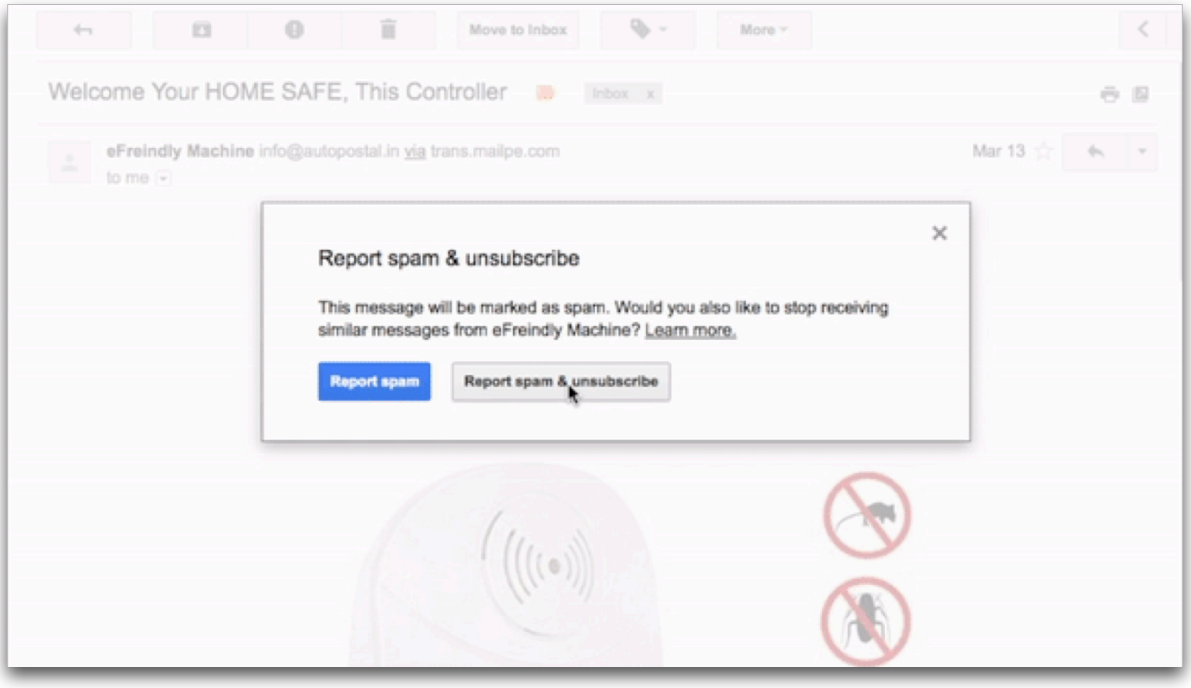


Figure 1: Gmail Flaw

The last image shows how Gmail behaves when you click the “Report Spam” button.

Gmail is giving us two options.

1. Report Spam
2. Report Spam & Unsubscribe.

What would you choose? Many naive users would go for the “Report Spam & Unsubscribe” option. Because they would think, that prevents them from receiving more spam emails.

But actually, that is a misconception.

If you click that button, you are actually going to receive more spam emails.

Back in 2003, the US government created the CAN-SPAM Act to fight spam. The U.S. Code § 7704 (a_5)[46] states the following.

[46] https://www.law.cornell.edu/uscode/text/15/7704#a_5

> clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender

So unsubscribe links are a requirement according to many countries anti-spam laws. However, spammers started to take advantage of those unsubscribe links.

First let us explain, how "unsubscribe" works.

In the email, the sender usually includes a header called "List-Unsubscribe[47]". This header is intended for the email clients

The header would look something like this. It usually contains an email address and/or a link to unsubscribe.

```
List-Unsubscribe: <mailto:optimumacesmart-42992-844-8840564-51eb8c824fc373e946a3da5a49afcdd2@usub.mailpe.com?
subject=Unsubscribe>, <http://panela.autopostal.in/optimumacesmart/?
p=smunsub&mid=844&uid=51eb8c824fc373e946a3da5a49afcdd2>
```

Figure 2: List-Unsubscribe

When you click the "Unsubscribe" link or button, the system notifies the sender saying that you are not interested in receiving any more emails from them.

So good… So far…

But, as we mentioned earlier, For a spammer, the primary source of email addresses are the Leaked Databases. HaveIBeenPwned.com[48] is a website that tracks the most popular data leaks. According to their website, almost 5 billion accounts are hacked from 280+ websites[49].

So, a spammer can easily find billions of valid email addresses online without any efforts.

For a spammer, the problem is not acquiring the valid email addresses. It's the active one.

[47] http://www.list-unsubscribe.com/
[48] https://haveibeenpwned.com/
[49] https://haveibeenpwned.com/PwnedWebsites

For example, a few years back all 3 billion accounts of Yahoo got hacked. Let's say a spammer send mails to all of those 3 billion users. Not all of them going to open their mails, right? Because plenty of them can be inactive accounts. The spammer wastes his time and money when he goes for all 3 billion.

So, for a successful spam campaign, a spammer need active email addresses. This is the reason why many spammers are actually spending their money to buy "active email address list" from other spammers.

When a genuine business include "unsubscribe" links, it means they are giving you the freedom to opt-out from their future promotional emails.

But when a spammer include "unsubscribe" links, it's for the exact opposite purpose.

So you should interpret that "Report Spam & Unsubscribe" button as "Who wants to receive more spam?" and when you click that button you are going like "Pick Me... Pick Me... Pick Me...".

If you really think spammers have moral principles, don't you think they would never spam you in the first place?

When it comes to spammers, every active email address is a golden goose. Do not think that the spammers are gonna let you walk away just because you are saying so. You may not get emails from the same email address, but we can assure you that this is not the end.

Further Reading: Back in 2007, Vircom[50] did an excellent research by interviewing 3 spammers and published a white paper titled "Why Spammers Spam[51]". Their answers are a goldmine for spam researchers.

Spam vs Phishing vs Spoofing

Spam

Spam mail usually have the following characteristics.

[50] https://www.vircom.com/
[51] https://www.yumpu.com/en/document/view/8160906/why-spammers-spam-vircomch

Unsolicited - You didn't give any permission to the sender to mail you.

Commercial - The sender is trying to sell you something.

Irrelevant - You are in your twenties. But the sender is trying to sell you viagra.

Bulk - You are not the only recipient of this mail.

We cannot classify a mail as spam based on only one characteristic. For example, when the mail's nature is only "Unsolicited" there could be other reasons too. e.g. You are sending feedback to a book author.

Phishing

Phishing mail usually have the following characteristics.

Deceitful - Phishing mails usually try to deceive you.

Incorrectness - Phishing mails usually hyperlink to the wrong URLs.

Example 1:

> From: paypal@gmail.com
>
> Sub: Your password is about to expire.
>
> Message:
>
> Hey there,
>
> Your password is about to expire. Please update the password here.
>
> https://www.paypal.com/update-password
>
> Regards,
>
> PayPal

Pay attention to the hyperlinked URL and the From email address.

Part	Type
comupdate-password.com	Original Domain
paypal	First level subdomain
www	Second level subdomain

Example 2:

Back in 2016, John Podesta email account got hacked and published on WikiLeaks. Here is the original conversation[52] between John Podesta and his IT team regarding the Phishing mail.

Whoever tried to reset the password, didn't use the link https://myaccount.google.com/security as suggested by Charles Delavan.

They actually used the original phishing link https://bit.ly/1PibSU0 (bit.ly is an url shortner. So it will redirect to the original link when someone clicks it)

This is the page where it redirects when you click it.

[52] https://wikileaks.org/podesta-emails/emailid/34899

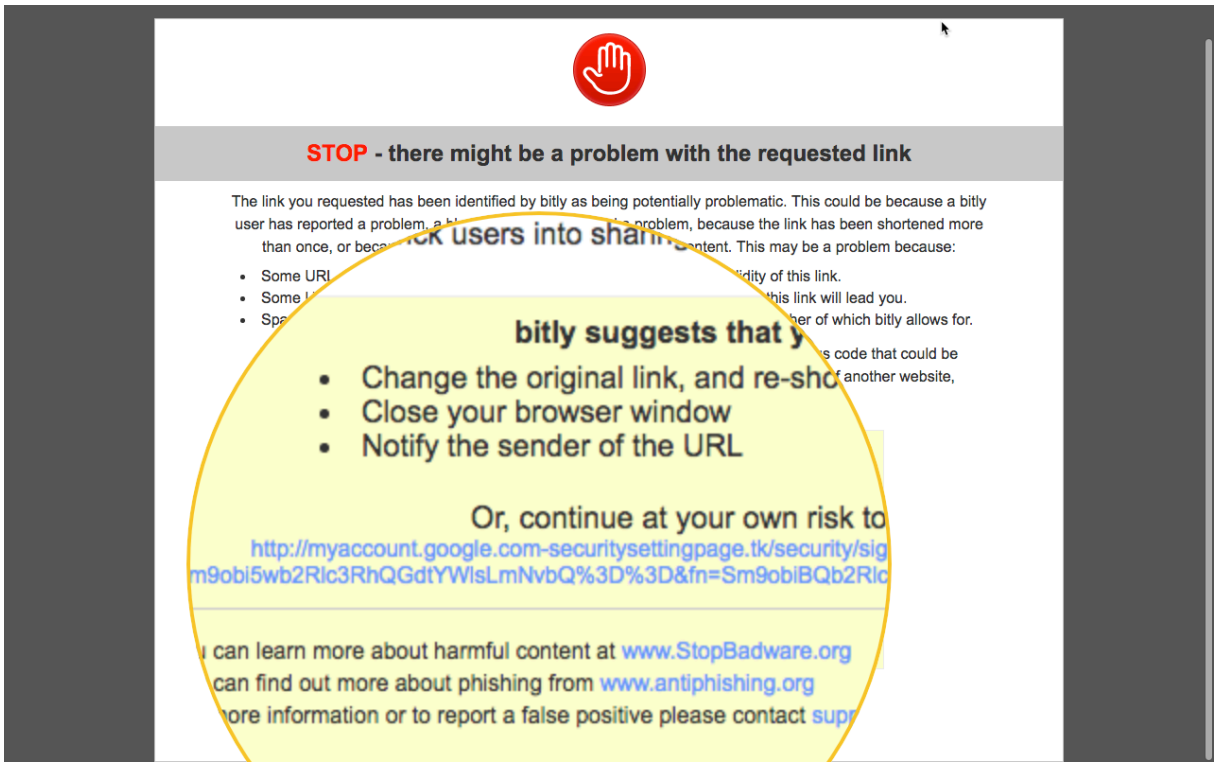


Figure 3: John Podesta Phishing Link

As you can see, you are being deceived there.

The term “Phishing” is a homophone of “Fishing” i.e. The scammer trying to catch unsuspecting victims (fish) by deceiving them.

When a victim falls for a “Phishing” mail, then it’s a result of “Human” error. Not “System” error.

ELI5 version: Someone invited a person named “Alex” to a party. Your name is “Alexa”. You show up with your ID card. The gatekeeper sees the name “Alex” on the list. He is convinced that you are Alex and let you in. The gatekeeper got deceived here. If he had paid more attention you would have been thrown out.

Spoofing

Unlike spam and phishing, Spoofing is a different ball game. It has one primary characteristic.

Forgery - The mails you receive are forged. e.g. The sender would use the "From" address like accounts@paypal.com, but the mail was not actually sent by paypal.

Today we have enough technologies to prevent email spoofing. But for Spam and Phishing, we are still relying on Machine Learning.

When it comes to Machine Learning (ML), there's always some room for "False Positives" until we have a pitch-perfect "Artificial Intelligence". When you have a pitch-perfect "Artificial Intelligence", email spam would be least of your concerns. e.g. Skynet taking over the world.

The following three mechanisms are widely used today to combat email spoofing.

SPF[53], DKIM[54] and DMARC[55]. We can talk about these in a later section.

ELI5 version: Someone invited a person named "Alex" to a party. Your name is "Alexa". You forge a new ID card for the person "Alex". You use that ID card to get in. In spoofing what you are doing is "Identity Theft". A much more serious crime than Phishing.

Note: Our system is bulletproof from all three. (Spam, Phishing and Spoofing)

[53] https://en.wikipedia.org/wiki/Sender_Policy_Framework
[54] https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail
[55] https://en.wikipedia.org/wiki/DMARC

Chapter 2: Email Overview

Mail Classifications

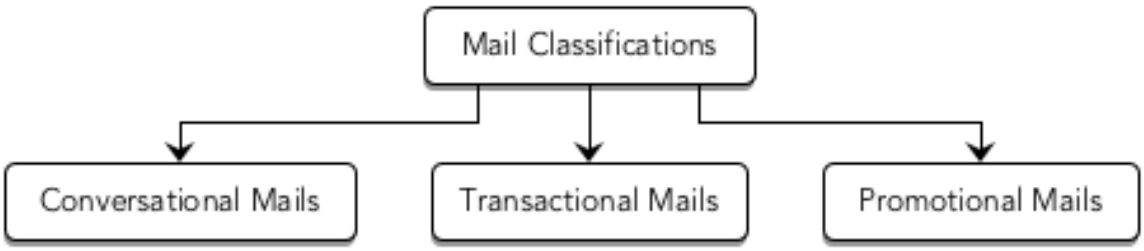


Figure 4: Mail Classifications

Conversational Mails

Conversational mails are all about you versus another human.

If the person who is sending you the mail is a human, then such mails go under conversational mails.

Small businesses sometimes depend on third-party services for conversational mails for security reasons. e.g. Google Apps

Transactional Mails

Transactional mails are all about you versus the website server.

These mails are automatically triggered when you interact with the website.

Think of it as a transaction between you and the website. The transaction can be money or data. You need to be notified for the transaction.

Transactional mails are usually sent out from the original website servers. i.e. Without depending on any third-party services. However, there are third-party transcational mail API services available too. e.g. AmazonSES, Mailgun, Postmark etc.

If you are the only Recipient of a mail sent by a website, then most likely it's a transactional mail.

Transactional Mail Examples:

- Mails triggered when you signup to a website.
- Mails triggered when you reset passwords.
- Mails triggered when you place an order.
- Mails triggered when you update your profile on a website.
- Mails triggered during certain website events. (Monthly Invoices, New friend request, New Facebook Likes, New Twitter Follower etc.)
- Confirmation Emails
- Welcome Emails
- Product Shipping Notices
- Purchase Receipts

Promotional Mails

Promotional mails are very different from transactional mails. When it comes to promotional mails, you are not the only recipient.

So promotional mails are all about website marketing team versus their users. Since you are one of their users, that includes you too.

Marketing team drafts the mail and then send it to all users in bulk.

Promotional mails usually contain tracking links.

Small businesses usually depend on third-party newsletter services to send out promotional mails. e.g. Mailchimp

This is because third-party services offer better tracking tools. e.g. how many people opened your emails, how many people clicked the links, how many people unsubscribed etc.

As per law, promotional mails require unsubscribe links. Transactional mails are not.

Notes

Both Transactional Mails and Promotional Mails are related to websites. So let's group them as "website related mails". Keep in mind, You don't need a website to send Transactional Mails and Promotional Mails.

e.g. A mobile app can send Transactional Mails with the help of third-party transactional mail services (e.g. AmazonSES) and it can send Promotional Mails via third-party newsletter services (e.g. MailChimp).

For simplification, we use the term "website related mails" to refer both Transactional Mails and Promotional Mails

Email Parts

An email can be divided into two parts

Part	Description
Envelope Part	This part is intended for mail handling servers.
Message Part	This is the part that gets displayed to the user.

Envelope Part

Figure 5: Envelope Part

Email is a hop-by-hop protocol. Meaning there can be multiple mail handling servers in between the sending server and the receiving server. e.g. Retrying server, Spam checking server, Virus scanning server etc.

So the SMTP protocol was designed to mimic our physical postal system. i.e. Anyone can be able to transmit emails for the domain they don't own.

SMTP stands for "Simple Mail Transfer Protocol". This is more like HTTP you see on browsers, but for email. Put it this way, HTTP is for the web and SMTP is for Email. SMTP was actually invented before the invention of HTTP. It is one of the oldest protocol and that is the reason why solving the problem is a hard thing. You cannot rewrite the protocol just to fix spam.

Message Part

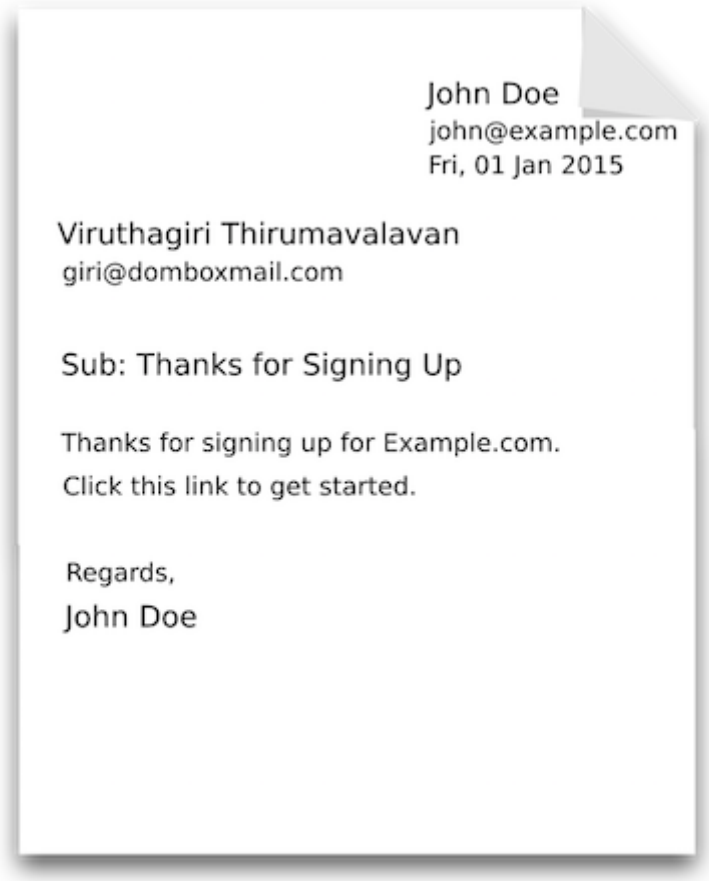


Figure 6: Message Part

This is the part that gets displayed to the user.

A message can have plenty of properties. But only the following five properties are “Very Important”.

From, To, Subject, Body and Date

All the above-mentioned properties can be extracted from the “Message Part”

Sample SMTP Chat

Sample mail conversation between the sending server and receiving server.

> mail.example.com Connecting to mail.domboxmail.com with its IP address
>
> domboxmail.com => 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> example.com => HELO mail.example.com
>
> domboxmail.com => 250 Hello, nice to meet you, mail.example.com
>
> example.com => MAIL FROM: <john@**example.com**>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <giri123$**example.com**@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => DATA
>
> domboxmail.com => 354 End data with <CRLF>.<CRLF>
>
> *example.com => From: John Doe <john@**example.com**>*
>
> *example.com => To: Giri <giri123$example.com@domboxmail.com>*
>
> *example.com => Date: Fri, 01 January 2015 16:02:43 -0500*
>
> *example.com => DKIM-Signature: s=selector123; d=**example.com**; .....*
>
> *example.com => Subject: Thanks for Signing Up*
>
> *example.com => Thanks for signing up for Example.com.*
>
> *example.com => Click <this link> to get started.*
>
> *example.com => Regards,*
>
> *example.com => John Doe*
>
> *example.com => .*
>
> domboxmail.com => 250 OK, message accepted for delivery: queued as 12345

> example.com => QUIT
>
> domboxmail.com => 221 Bye

“Envelope Part” is represented in “Normal Font”

“Message Part” is represented in “Italics Font”

The Four Domains

Our system deals with the following 4 domains

Domain	Can be extracted from
Envelope Domain	MAIL FROM: <john@**example.com**>
Dombox Domain	RCPT TO: <giri123$**example.com**@domboxmail.com>
Message Domain	From: John Doe <john@**example.com**>
Signature Domain	DKIM-Signature: s=selector123; d=**example.com**; .....

Note: “Dombox Domain” refers to the domain found between the “$” symbol and “@” symbol and it’s applicable only to the boxes found in “Domboxes” group {Refer chapter 4}. Some people may be confused with our official domain “domboxmail.com”. In such situations use the term “Box Domain” instead of “Dombox Domain”.

The Three Domains

“Dombox Domain” is something we are introducing and it’s applicable only to our system.

All other email systems on the internet deal with only the other three domains.

i.e. Envelope Domain, Message Domain and Signature Domain.

Just for the sake of this document, let’s classify the mails into three types.

1. Excellent Mails

2. Normal Mails
3. Abnormal Mails

Note: The following few screenshots are captured in Gmail. Gmail use different terms for those domains.

Dombox Term	Gmail Term
Message Domain	from*
Envelope Domain	mailed-by
Signature Domain	signed-by

* Gmail use full “Message From” address there

Excellent Mails

We can call a mail as “excellent” when all three domains are the same.

Excellent Mail Example: Stripe

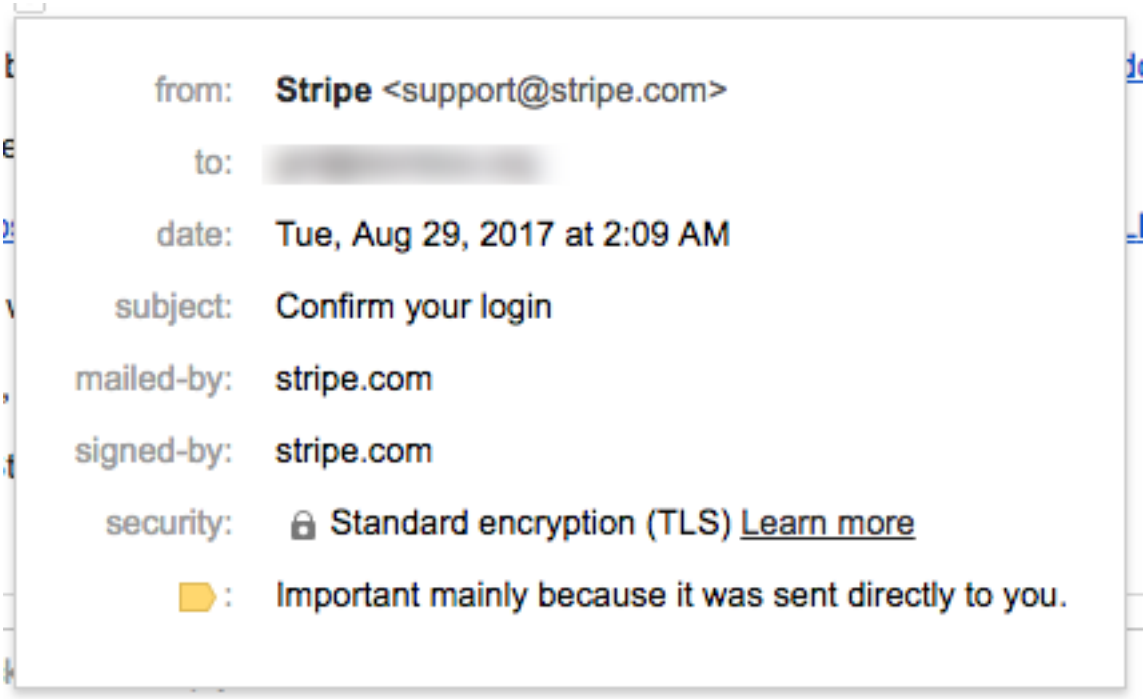


Figure 7: Stripe

Domain	Value
Message Domain	stripe.com
Envelope Domain	stripe.com
Signature Domain	stripe.com

Normal Mails

We can call a mail as “normal” if only the “envelope domain” is different.

The “envelope domain” can be different when third party services used for sending emails. So we consider such emails as Normal. e.g. Mailchimp, Sendgrid, AmazonSES

Normal Mail Example 1: Mailchimp

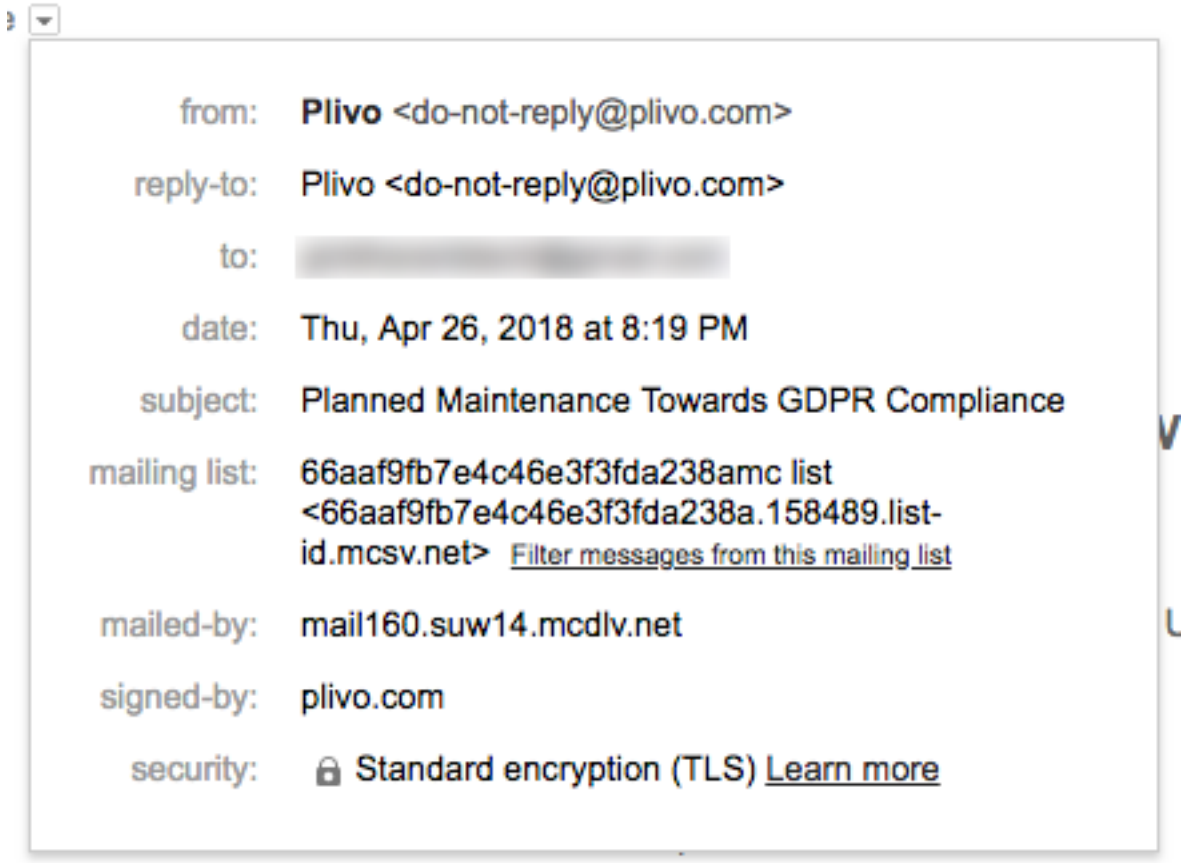


Figure 8: Mailchimp

Domain	Value
Message Domain	plivo.com
Envelope Domain	mail160.suw14.mcdlv.net*
Signature Domain	plivo.com

* mcdlv.net is one of the sending servers of MailChimp

Normal Mail Example 2: Sendgrid

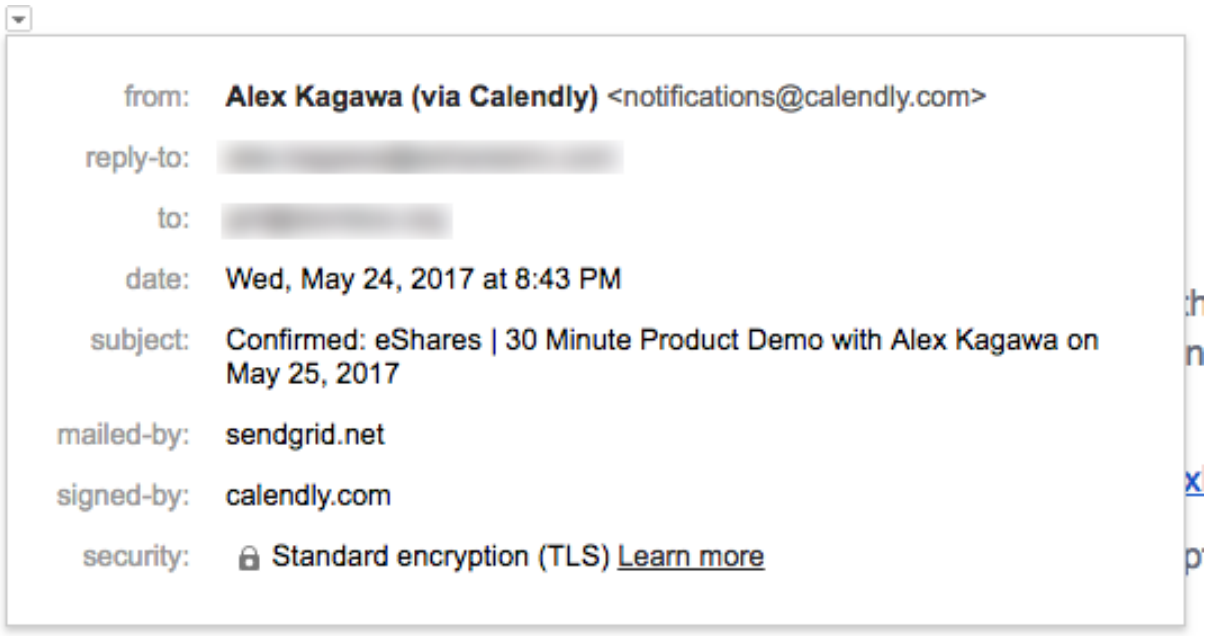


Figure 9: SendGrid

Domain	Value
Message Domain	calendly.com
Envelope Domain	sendgrid.net
Signature Domain	calendly.com

Normal Mail Example 3: AmazonSES

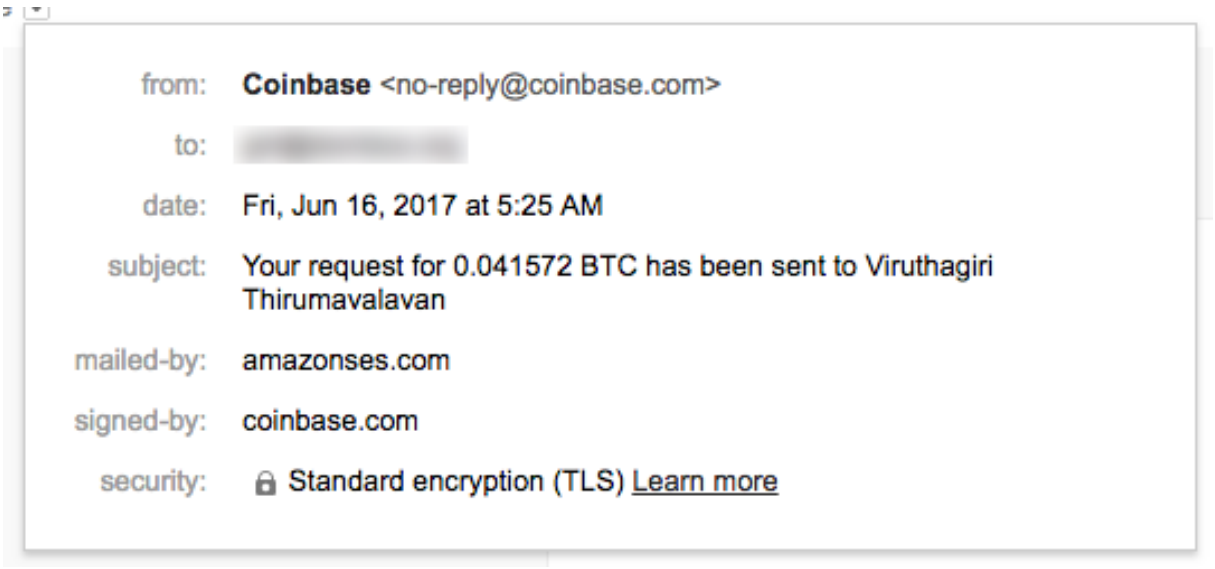


Figure 10: AmazonSES

Domain	Value
Message Domain	coinbase.com
Envelope Domain	amazonses.com
Signature Domain	coinbase.com

Abnormal Mails

We can call a mail as “abnormal” when the “signature domain” doesn’t match the “message domain”

The whole purpose of the signature is to make sure the message has not been modified in transit.

Thus it should be signed by the “Message Author”. i.e. Where it originates => The “Message From” domain

When the “Signature Domain” doesn’t match the “Message Domain”, Gmail adds a “via” text

So the user can understand that the message has not been modified in transit, but someone else signed the message.

Abnormal Mail Example: MailChimp

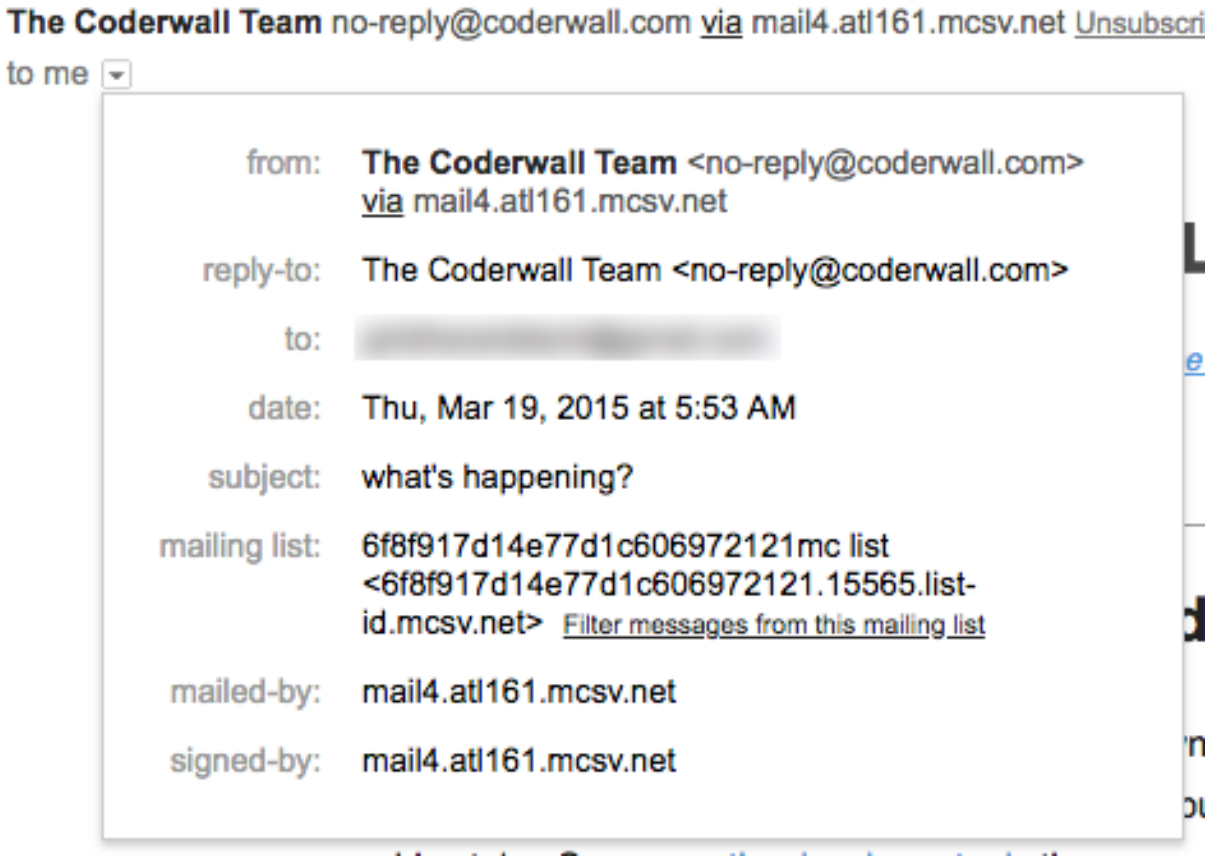


Figure 11: Mailchimp

Domain	Value
Message Domain	coderwall.com

Domain	Value
Envelope Domain	mail4.atl161.mcsv.net*
Signature Domain	mail4.atl161.mcsv.net*

* mcsv.net is one of the sending servers of MailChimp

Chapter 3: Solution Overview

For the sake of this document, We are gonna call our new email system as “Email 2.0”. The current email system (e.g. Gmail) should be considered as “Email 1.0”

Our system doesn’t have the “spam” folder. And it makes your emails more organized.

We believe, the only way to kill spam is to never accept the spam mail at all.

i.e. The system should be able to reject the spam mail instantly.

Why Mail Rejection can kill email spam?

Receiver’s Perspective

The problem with spam filters is that, it has no idea about what’s going on OUTSIDE the email system.

i.e. A spam filter may mark an incoming mail as genuine if the sender’s email address found in the Address Book. But for others, it has to rely on machine learning algorithms to detect mail genuineness.

Sender’s Perspective

Spammers have no idea what’s going on INSIDE the email system.

i.e. A spammer has no idea whether the mail is marked as spam or not.

Let's pretend that you are a budding film director. You would like to bring Johnny Depp on board for your new film. So you send him an email. If you don't hear anything from him for a while, then you are gonna write a follow-up mail.

Now, what if your first mail get rejected with an error message like "Unauthorized Sender"?

Would you still write your follow-up mail? No... right?

That's because you know it's a dead end.

Now apply this scenario to spammers. Spammers are living with hope. They are hoping atleast one of their receivers gonna read their mails and buy whatever they are selling. A 2008 study shows that spammers get only One response per 12,500,000 emails[56], yet that's still profitable for them.

Spammers send millions of spam mails to unknown people. They are wasting their time and resources if they go after invalid and inactive email addresses. Also note that many spammers buy targeted email lists from other spammers. Thus, they need to maintain fresh and active email addresses in order to sell it to other spammers.

So when mails get rejected with an error message, spammers gonna remove your email address from their email list. That's because your email address is a dead end for them.

Problem with Mail Rejection

Rejecting spammer mails comes with a big complication. A system must be able to clearly identify the spammers. If you reject mails that are from Genuine Senders, then your system is completely flawed.

You don't wanna lose mails from handful of Genuine Senders. That's the whole purpose of having spam filters, right?

[56] https://www.techradar.com/news/internet/computing/spam-gets-1-response-per-12-500-000-emails-483381

Create an Account

Let's create an account in our mail system. Nothing fancy here. Let's pretend that we get the following new email address once we complete the signup process.

Email Address: giri@domboxmail.com

This email address is equivalent to a gmail.com address. i.e. It can accept mails from anyone.

At this stage, our system should be treated as Email 1.0 [And yes, we are gonna have the spam folder at this stage]

This is how our mail system looks like now.

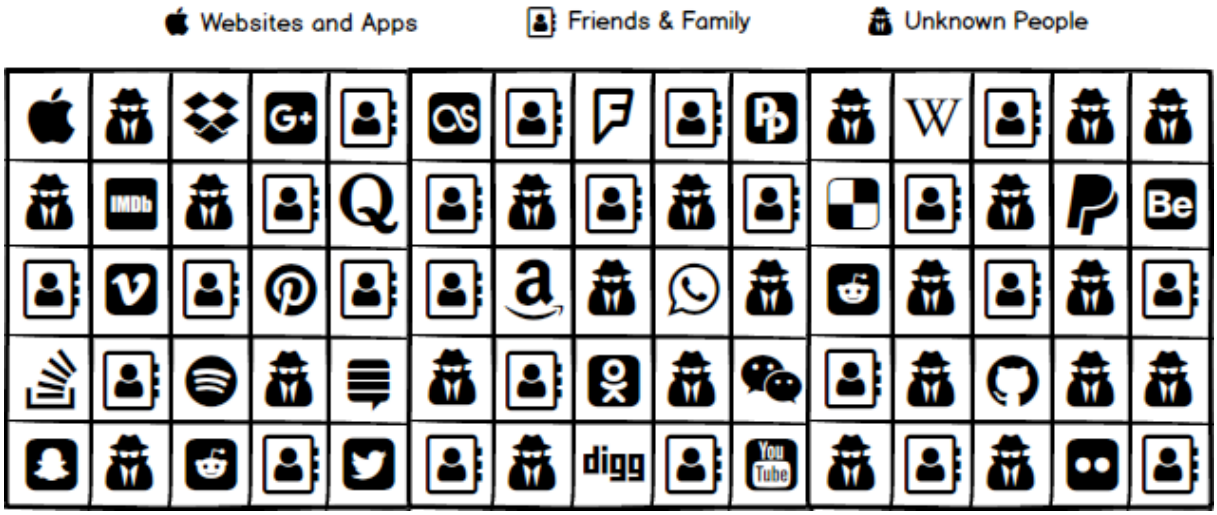


Figure 12: Normal Mail System

Unique Solution

> Isolate, Restrict and Inject

We solve the email spam problem in three phases. Isolation, Restriction and Injection

We have two kinds of mailboxes. (A) Normal Mailboxes (B) Isolated Mailboxes

Isolation:

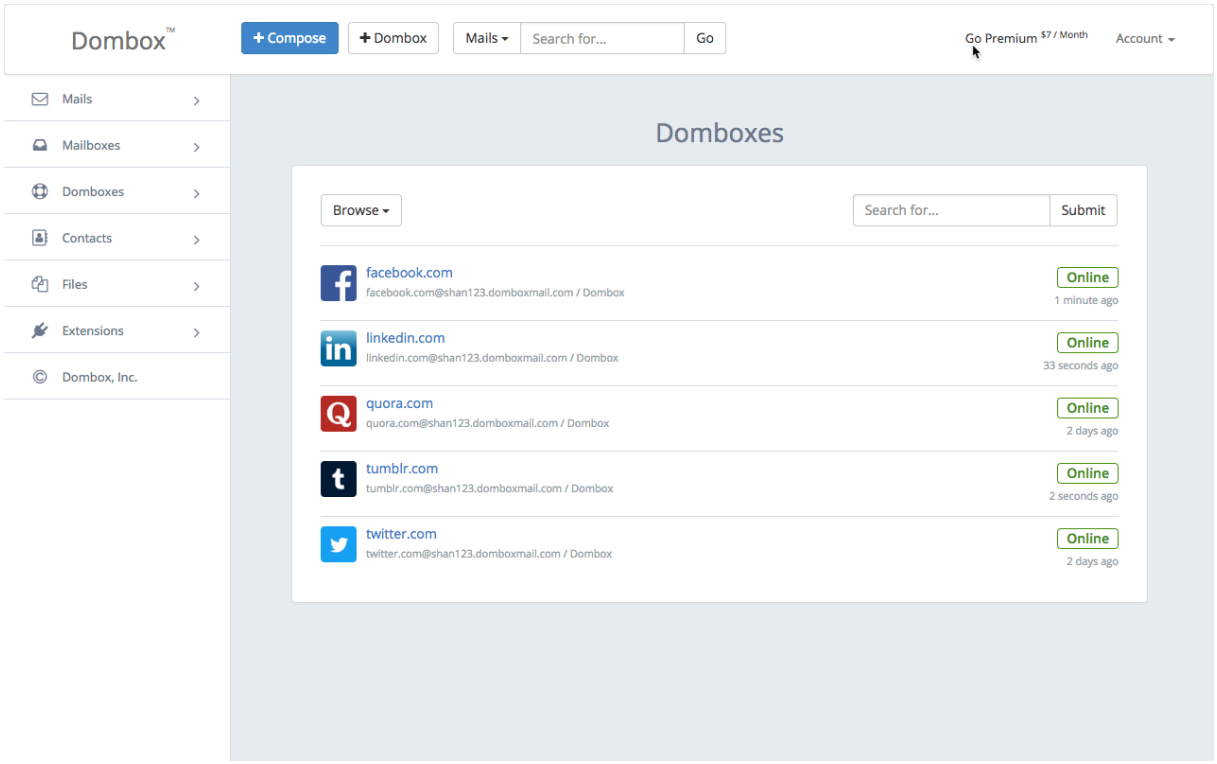


Figure 13: Isolation

This phase deals with Isolated Mailboxes.

In this phase all the websites you signup are isolated. An isolated mailbox will be given to each website you signup. Only that particular website can send emails to that isolated mailbox by default.

However, that particular website can whitelist certain third-party domains in their DNS to send mail to their isolated mailbox.

All websites have the exclusive unrestricted privilege to send emails to their “Isolated Mailbox”.

Isolated mailboxes are called “Domboxes” in our system. Dombox stands for Domain-based Isolated Mailbox. It’s powered by something we call “i-mail address aka. isolated-mail address”.

This is the end result after completing the Isolation phase.

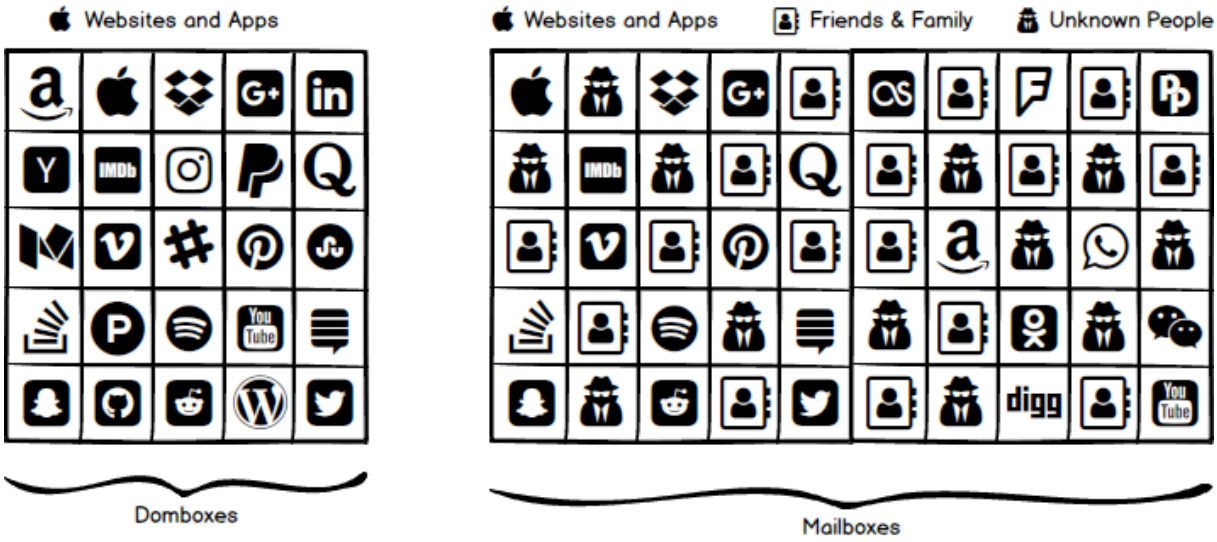


Figure 14: Isolation Phase

Note: “Normal Mailboxes” still can be able to accept mails from websites and app at this stage. That’s why Mailboxes part contains website and app icons in the last figure.

Restriction:

This phase deals with only Normal Mailboxes. Normal Mailbox addresses are called “e-mail address” in our system.

Note: All i-mail addresses can be called as “e-mail address”. But not all e-mail addresses can be called “i-mail address”.

All “websites related mails” are already offloaded to Domboxes. So this phase deals with only the “conversational mails”

A normal mailbox works exactly the same way just like your @gmail.com mailbox. However, our normal mailboxes come with an option called “Restricted Mode”.

When enabled it allows emails only from the contacts found in your “Address Book”

Since we already isolated website related emails with “Isolated Mailboxes”, normal mailboxes are only about real conversational emails you get from your friends, family or someone you already know. So when you enable “Restricted Mode”, it’s more like hanging a board with a sign “Authorized Personnel Only”

Keep in mind, you cannot have “Restriction” without “Isolation”. Because we offload all website related emails to “Isolated Mailboxes” and then keep only the conversational emails in “Normal Mailboxes”

Note: You can use third party email addresses like @gmail.com in our system for Normal Mailboxes. However for “Isolated Mailboxes” you have to use our i-mail address which ends with @domboxmail.com.

If you are gonna use this phase, be sure to offload all website related mails (i.e. Promotional Mails and Transactional Mails) to Domboxes and only keep the Conversational Mails in the Mailboxes.

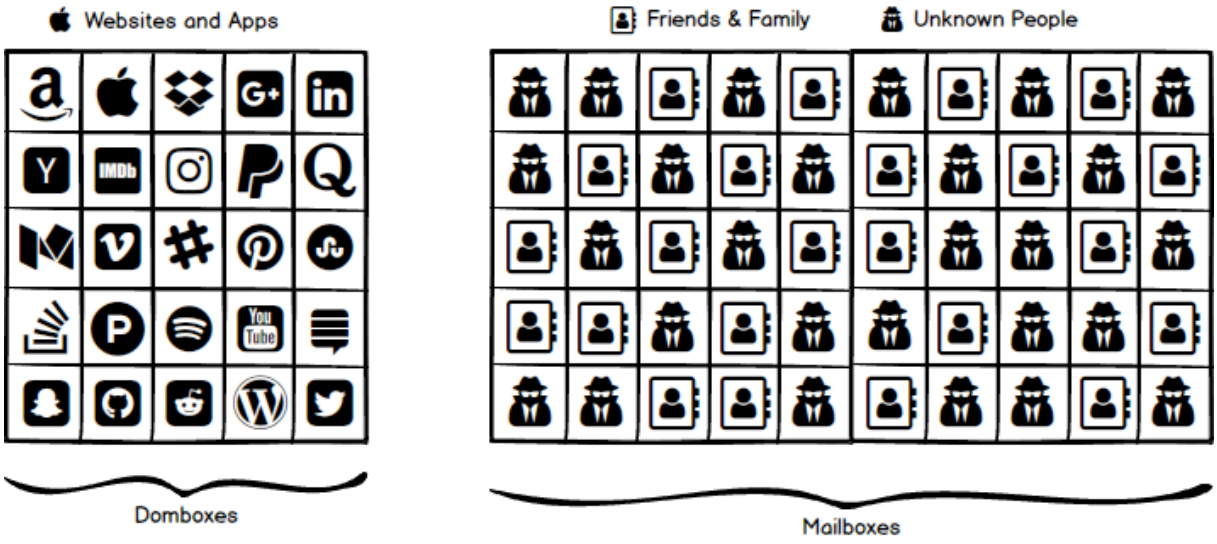


Figure 15: Before Restricted Mode

Pay attention to the Mailboxes part. No website and app icons there. Only human icons available now [Which means Conversational Mails].

This is the end result, once you activate “Restricted Mode”.

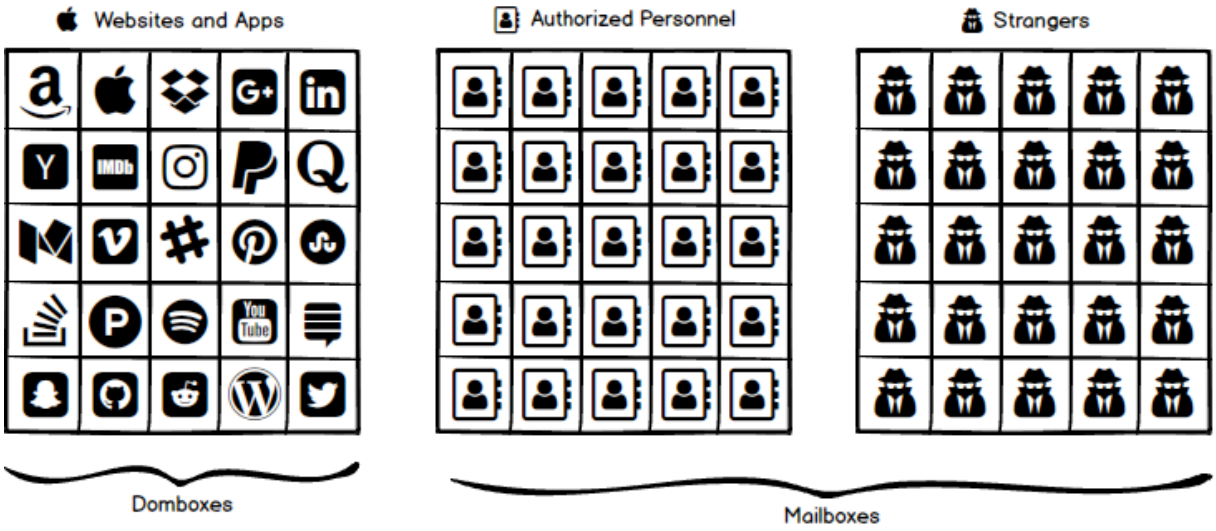


Figure 16: After Restricted Mode

Injection:

This phase only deals with “Strangers” and rely on Challenge/Response mechanism to detect spam mails.

This phase contains the following methods.

Method 1: Intro via a Mutual Contact

Method 2: CAPTCHA

Method 3: Phone Number Validation

Method 4: Proof-of-Work (PoW)

Method 5: Attention Fee

There are many methods available in this phase. But the one that would work for everyone is the CAPTCHA method.

So, We are gonna send an email back asking the sender to fill CAPTCHA. This type of system is known as Challenge/Response mechanism and it was first introduced in 1997.

The reason C/R mechanism not popular even after two decades is because

All other solution sends challenge mails even to bulk mailers like MailChimp. So bulk mailers cannot respond to challenges. [We solved this issue with Domboxes. Domboxes provides exclusive unrestricted privilege for domains to send mails to their Dombox.]

Challenge mails are heavily suffering from backscatter attacks. i.e. Bad guy forge the mail like it's coming from president@whitehouse.gov. Challenge mails are being sent to president@whitehouse.gov

Injection phase applicable only for Conversational Mails.

Conversational Mails can be termed as MX-to-MX mails. We primarily check whether the incoming mails coming from the MX Record IP addresses or the SPF record IP addresses. If Yes, then we are gonna send our challenge mails back. If not, we are gonna reject the mails immediately.

The crystal clear way of knowing "conversational mails" from "website related mails" is what makes our system click.

To summarise,

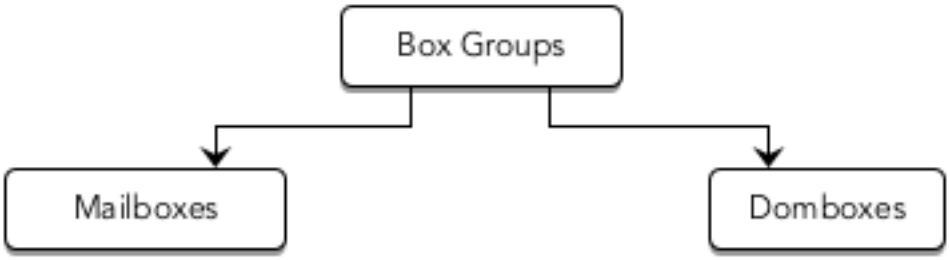
Isolation for websites

Restriction for friends, family, colleagues and acquaintance (i.e. People found in your Address Book aka. Authorized Personnel)

Injection for Strangers

Chapter 4: Box Groups

The term "box" refers to any mailbox that has the capability of receiving emails.



Normal Mailboxes Aka. Mailboxes

This works exactly like other mail services. e.g. Gmail. When a user signup to our mail service, the user will get one normal mailbox for free.

This “one normal mailbox” is called “Primary (P)” Mailbox in our system.

The boxes found in this group can accept mails from anyone including spammers.

In our system “Normal Mailboxes” should be used only for “Conversational Mails”.

Address structure:

> local-part@domain

e.g. johndoe@domboxmail.com

The addresses found in this category are called “email address” or “e-mail address”. These addresses are also known as “Mailbox Address”

Isolated Mailboxes Aka. Domboxes

Dombox is the short form for “Domain-based Isolated Mailbox”

Users are gonna create a separate mailbox for each domain. Each of this separated (i.e. Isolated) mailbox is called Dombox

The internet as we know it, is powered by “Normal Mailboxes”. Normal Mailboxes are nothing but “Shared” Mailboxes. Domboxes are “Dedicated” Mailboxes.

The boxes found in this group can accept mails only from the “Box Domain” and its “SAD domains”. {Note: SAD Domains will be explained in a later section}

Isolated Mailboxes should be used only for Transactional and Promotional Mails.

Email address structure:

> Domkey$BoxDomain@ReceiverDomain

e.g. giri123$twitter.com@domboxmail.com

The addresses found in this category are called “imail address” or “i-mail address” which stands for “isolated mail address”. These addresses are also known as “Dombox Address”

A user can have unlimited Domboxes

All emails you receive from websites fall under either Transactional or Promotional Mails category.

The internet has 332 million[57] domains as of 2018. But the user is gonna create Domboxes only for the site he/she about to signup. If the user signup to 1 website every week, that will be around 52 websites every year. Domboxes doesn’t have to be created manually.

A Dombox can be created in three ways.

1. Manually {Refer Chapter 9}
2. Via Teleport button {Refer Chapter 10}
3. Via Telescribe button. {Refer Chapter 12}

Dombox email address is compatible with 99.99% of the domains in the world.

Dombox email address structure splits the “local-part” into two parts via Dollar symbol and the Dollar symbol is a perfectly valid character in the local-part.

Domkey is required to generate a Dombox

Note: Only the “Box Domain” and its “SAD Domains” can **write** emails to the “Isolated Mailbox”. Only the consumer can **read** and **delete** emails from the “Isolated Mailbox”.

[57] https://blog.verisign.com/domain-names/verisign-q4-2017-domain-name-industry-brief-internet-grows-332-4-million-domain-name-registrations-fourth-quarter-2017/

Questions

Are you trying to re-invent email?

Just because there is a $ symbol in our email address structure doesn't mean we re-invented the email.

hello+world@gmail.com

That's a valid Gmail address. You can't say Google re-invented the email by using the + symbol. Can you?

In our email address, we use the $ symbol which is a perfectly valid character[58] in the email address local part according to email standards.

Whether you believe it or not, the following email address is a perfectly valid email address.

> #!$%&'*+-/=?^_`{}|~@example.org

We are using the $ symbol, so our system and third-party websites can recognize our isolated mailbox address easily.

As programmers, we use Terminal at least once a day. We get to see the Dollar symbol every day in the Terminal. So for us, Dollar symbol makes more sense while compared to other symbols like +, % etc. That's the reason we chose the $ symbol.

So, no... We are not trying to re-invent the email. We are just trying to fix the "email spam" without breaking the existing email design.

Domkey

Domkey is the short form for "Dombox Global Keyword". {Heads Up! Its "Dombox Global Keyword". Not "Domain Global Keyword"}

Domkey will be the same for all user created Domboxes.

Domkey should be a unique string just like a username.

[58] https://en.wikipedia.org/wiki/Email_address#Local-part

Domkey should be an alphanumeric string.

Domkey must be set before creating your first “Dombox”

Domkey can be set only once for an account and cannot be changed later.

Domkey cannot be one of your “Normal Mailbox” local-part. i.e. If you have an email address like johndoe@domboxmail.com, then you can’t have “johndoe” as value for Domkey

Address Structures

In late 2017, we acquired the .com zone file[59] from Verisign and analyzed the character length of 130 million .com domains.

The next table shows the results.

Length	Count	Length	Count	Length	Count
1	3	22	2033228	43	6029
2	1291	23	1595203	44	4854
3	47702	24	1224185	45	4015
4	998564	25	928130	46	3119
5	4591414	26	704339	47	2567
6	7112103	27	522309	48	2089
7	7377277	28	384176	49	1649
8	8263424	29	285567	50	1568
9	9114806	30	209808	51	1199
10	9973238	31	151509	52	1122
11	10222313	32	826398	53	989
12	9983689	33	81414	54	844

[59] https://www.verisign.com/en_US/channel-resources/domain-registry-products/zone-file/index.xhtml

Length	Count	Length	Count	Length	Count
13	9531235	34	60257	55	698
14	8761398	35	45191	56	672
15	7765227	36	34549	57	604
16	6759578	37	25480	58	539
17	5836950	38	19751	59	523
18	4840956	39	15022	60	599
19	3947458	40	11893	61	446
20	3229439	41	9287	62	410
21	2568350	42	7424	63	695

Total .com Domains: 130136765 (~ 130 million)

In a URL, the parts that are separated by the dot are called “Labels”. For example, www.youtube.com contains 3 labels. i.e. www, youtube and com. A label can have a maximum of 63 characters.

In www.youtube.com, “youtube” is the second level domain. When you try to register a .com domain you need to choose this second level domain. The zone file contains only the second level domains. i.e. Without the “.com” part. {Having .com 130 million times increases the file size a lot}

For instance, only 3 “.com” domains are registered in the world so far that has 1 Character Length. They are q.com, x.com and z.com. So you will see 3 results for 1 character domain in the table.

Isolated mailboxes will actually have two different email address structures. The second address structure will act as an alias.

1. Dollar-based
2. Subdomain-based

Dollar-based

I-Mail Address Structure : Dollar-based

Domkey	$	Dombox Domain	@	Receiver Domain

Examples

giri123	$	example.com	@	domboxmail.com
giri123	$	google.com	@	domboxmail.com
giri123	$	facebook.com	@	domboxmail.com
giri123	$	twitter.com	@	domboxmail.com
giri123	$	yahoo.com	@	domboxmail.com

Figure 17: Dollar-based

> Domkey$BoxDomain@ReceiverDomain

e.g.

testkey123$twitter.com@domboxmail.com

testkey123$linkedin.com@domboxmail.com

testkey123$adobe.com@domboxmail.com

There is one problem with this Dollar-based address structure.

The maximum allowed characters in email address local-part are 64 characters. i.e. Before the @ symbol

So our Dollar-based structure is not compatible with all domains.

Note: Don't get confused with the "Label" maximum characters we explained in our www.youtube.com example. That's 63 characters and that's not related to the email address.

Subject	Structure	Example	Max Characters
Domain	{label}.{label}	youtube.com	63 {Each Label}
Email Address	{local-part}@{domain}	jeff@amazon.com	64 {Local Part}

We are planning to allocate 30 characters for the {Domkey}.

$ symbol takes 1 character.

That means only 33 characters are left for {BoxDomain}

Item	Characters Allocated
Domkey	30
Dollar Symbol	1
BoxDomain	33
Total	**64**

We need to make sure 33 characters enough for BoxDomain.

Remember... Zone file truncated the .com part. That's 4 characters. That means 29 characters. So let's divide our research data you see in the table into two parts.

1. Second level domains that are less than or equal to 29 characters
2. Second level domains that are more than 29 characters

Second level domains that are less than or equal to 29 characters: 128,603,552 (~ 128.5 Million i.e. 98.82%)

Second level domains that are more than 29 characters: 1,533,213 (~ 1.5 Million i.e. 1.17%)

These 1.17% domains are most likely not genuine businesses. But it's still our responsibility to make sure our isolated mailbox address is compatible with almost every domain in the world.

For these 1.17% of the domains, we are introducing a second address structure. This address structure is subdomain-based.

The second structure is an alias. It should be used only when you have issues with the main address structure. e.g. Some poorly coded websites might consider the $ symbol as invalid character.

Subdomain-Based

I-Mail Address Structure : Subdomain-based

Dombox Domain	@	Domkey	.	Receiver Domain

Examples

example.com	@	giri123	.	domboxmail.com
google.com	@	giri123	.	domboxmail.com
facebook.com	@	giri123	.	domboxmail.com
twitter.com	@	giri123	.	domboxmail.com
yahoo.com	@	giri123	.	domboxmail.com

Figure 18: Subdomain-based

> BoxDomain@Domkey.ReceiverDomain

e.g.

twitter.com@testkey123.domboxmail.com

linkedin.com@testkey123.domboxmail.com

adobe.com@testkey123.domboxmail.com

The {BoxDomain} now can have the full 64 characters for domain

Since we are allowing 64 characters in the local-part we can divide the research into two parts.

1. Second level domains that are less than or equal to 60 characters

2. Second level domains that are more than 60 characters

Note: we allocated 4 characters for ".com"

Second level domains that are less than or equal to 60 characters: 130,135,214 (99.998%)

Second level domains that are more than 60 characters: 1551 (0.001%)

So this structure is compatible with 99.99% domains

Note: We analyzed only the .com domains. Although .com, .net and .org are the most popular TLDs, there are actually 1500+ TLDs[60] out there as of 2018

Questions

If the second structure is compatible with 99.99% of the domains, why do we need the first one? Why not just stick with the second?

Well… We need the first structure to provide good user experience.

Since the first address structure starts with the {Domkey}, we can offer autocomplete feature.

When a user trying to login to a third party website, instead of typing the whole email address like "testkey123$twitter.com@domboxmail.com", the user now can type "testkey123$" and then press tab.

Our autocomplete feature will behave like this.

[60] http://stats.research.icann.org/dns/tld_report/

Form Email Field => Alphanumeric characters + The dollar symbol + Tab key press = capture the current domain and then autocomplete the isolated email address

Although we can add "Autocomplete" feature in subdomain-based structure too, it won't be as good as Dollar-based structure.

Is 30 characters enough for {Domkey}?

Gmail username has a maximum character limit of 30 characters.

As of April 2018, Gmail has 1.4 billion[61] monthly active users and the 30 characters limit works for them. So we think 30 characters are enough for {Domkey} too.

Is $ a valid character in the email address?

Yes... It's perfectly valid. Stop asking that question.

What are the characters allowed in the isolated mailbox address?

{Domkey} - Can contain only alphanumeric characters. 30 characters maximum.

{BoxDomain} - Can contain only alphanumeric characters, dashes/hyphens (-) and dots.

Also note {BoxDomain} will be the main domain.

For example, if you try to create a box for https://del.icio.us the box will be created for "icio.us" because that's the main domain.

[61] https://money.cnn.com/2018/09/20/technology/google-gmail-scanning/index.html

Chapter 5: Architecture

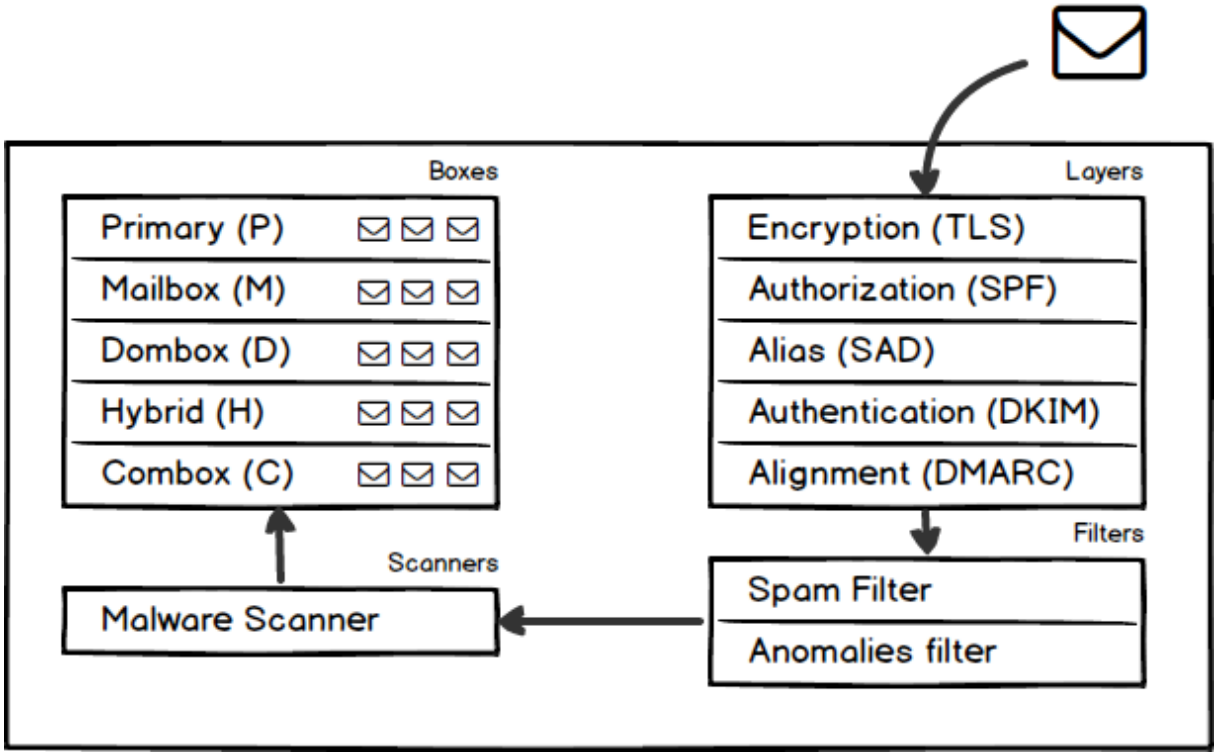


Figure 19: Architecture

Our system contains 4 major components

Component	Description
Layers	This component contains 5 Layers. Spam mails usually get caught in one of these layers
Filters	This component contains 2 Filters. Spam Filter & Anomalies Filter. We need “Spam Filter” for backward compatibility. i.e. Some users may wanna use our system as traditional mail system [Email 1.0]. Anomalies Filter will be explained in a later section

Component	Description
Scanners	This component contains virus scanners
Boxes	This component contains 5 Box Types. Each box type is designed for a different purpose.

Chapter 6: Layers

All incoming mails will be passed through these 5 layers. Spam emails usually get caught in one of these layers. So the mail will be rejected instantly.

Layer	Description
Encryption Layer	Checks whether the mail is encrypted.
Authorization Layer	Checks whether the “Sending IP” is authorized to send mails for the “Envelope Domain”
Alias Layer	Checks whether both “Envelope and Message Domain” are an alias for the “Dombox Domain”
Authentication Layer	Checks whether the mail is digitally signed
Alignment Layer	Checks whether the domains are aligned

Primary Subject

Layer	Subject	Record Path
Encryption Layer	-	-
Authorization Layer	Envelope Domain	*envelope*domain.com

Layer	Subject	Record Path
Alias Layer	Dombox Domain	_sad.*dombox*domain.com
Authentication Layer	Signature Domain	selector._domainkey.*signature*domain.com
Alignment Layer	Message Domain	_dmarc.*message*domain.com

Technical Names

Layer	Name	Description
Encryption Layer	TLS	Transport Layer Security
Authorization Layer	SPF	Sender Policy Framework
Alias Layer	SAD	Sender Alias Domains
Authentication Layer	DKIM	DomainKeys Identified Mail
Alignment Layer	DMA	Domain-based Message Authentication, Reporting and Conformance

Encryption Layer

Checks whether the mail is encrypted.

Technical Name: Transport Layer Security (TLS)

Possible Results: Pass or Fail

Pass - Encrypted

Fail - Not Encrypted

Note: We are talking about the secure commnication between the sending server and the receiving server here. We are not talking about end-to-end encryption.

Authorization Layer

Checks whether the “Sending IP / Client IP” is authorized to send mails for the “Envelope Domain”.

Technical Name: Sender Policy Framework (SPF)

Possible Results: Pass or Neutral or Fail

Pass - Authorized

Neutral - Not Configured. So neither Authorized nor Unauthorized

Fail - Unauthorized

Sample SPF Record Query

Note: The SPF record will be fetched from the **Envelope Domain**

Domain	Can be extracted from
Envelope Domain	MAIL FROM: <mark@facebook.com>

Record Path: envelopedomain.com

```
GiriMac:Prototype giri$ dig +short txt facebook.com
"v=spf1 redirect=_spf.facebook.com"
GiriMac:Prototype giri$ dig +short txt _spf.facebook.com
"v=spf1 ip4:69.63.179.25 ip4:69.63.178.128/25 ip4:69.63.184.0/25 ip4:66.220.144.128/25 ip4:66.220.155.0/24
 ip4:69.171.232.0/24 i" "p4:66.220.157.0/25 ip4:69.171.244.0/24 mx -all"
GiriMac:Prototype giri$
```

Figure 20: SPF Query

Alias Layer

Checks whether the “Envelope and Message Domain” are an alias for the “Dombox Domain”

Technical Name: Sender Alias Domains (SAD)

Possible Results: Pass (FakePass, DirectPass, IndirectPass)

FakePass - Alias Layer applicable only for “Domboxes”. So if the incoming mail is to the boxes found in “Mailboxes” group, then the result is set to “FakePass” for consistency {Refer “Mail Score” in Chapter 7}.

DirectPass - When the “Envelope and Message Domain” are the same as “Dombox Domain”. In this case no need to check for SAD Record

IndirectPass - When the “Envelope and Message Domain” are not the same as “Dombox Domain”, but passed via SAD record.

Note: If the Alias Layer result is “Fail”, then the mail will be rejected. So the only possible result for “Alias Layer” is “Pass”

Alias layer is divided into two sub layers

Layer	Description
Envelope Layer	Checks whether the “Envelope Domain” is an alias for the “Dombox Domain”
Message Layer	Checks whether the “Message Domain” is an alias for the “Dombox Domain”

Alias Layer is all about 3 domains. Dombox Domain (Primary Subject) compares itself with “Envelope Domain” and “Message Domain”

Keep in mind, this layer consists of two checks. One for the “Envelope Layer” and One for the “Message Layer”. Even if one Layer result is “Fail”, then the mail will be rejected.

The SAD Record is explained in the next section

Sender Alias Domains

We created an isolated mailbox for amazon.in and the box address looks like this => giri123$amazon.in@domboxmail.com

This box can accept mails only from amazon.in by default

To allow mail from jeff@amazon.com to amazon.in box, amazon.in should have the following SAD record in _sad.amazon.in

> v=sad1 amazon.com:r+b example.com:s+e -all

Note: We always check the SAD record in the “Dombox Domain”. The “Dombox Domain” can be extracted from the Isolated Mailbox address

giri123$amazon.in@domboxmail.com => amazon.in

SAD Configuration

A SAD record can have multiple domains and each domain can have a configuration.

> {Domain}:{Relaxed or Strict}+{Envelope Mode or Message Mode or Both}

Mode	Description
Relaxed (r)	Exact domain and its subdomains are allowed (Default)
Strict (s)	Exact domain only allowed.
Envelope Mode (e)	Domain is allowed only in the “Envelope From” (Default)
Message Mode (m)	Domain is allowed only in the “Message From”
Both Mode (b)	Domain is allowed in “Envelope From” as well as “Message From”

So, “v=sad1 example.com -all” is equivalent to “v=sad1 example.com:r+e -all”

SAD Examples

ED = Envelope Domain, MD = Message Domain, DD = Dombox Domain

Box created for facebook.com (DD), mails are carried by third-party newsletter service mailchimp.com (ED) for the domain facebook.com (MD). In this case, add the following record in “Dombox Domain” DNS.

> _sad.facebook.com => “v=sad1 mailchimp.com -all”

Box created for facebook.com (DD), mails are carried by facebook.com (ED) for one of their product instagram.com (MD). In this case, add the following record in “Dombox Domain” DNS.

> _sad.facebook.com => “v=sad1 instagram.com:r+m -all”

Box created for facebook.com (DD), mails are carried by third-party newsletter service mailchimp.com (ED) for one of Facebook product instagram.com (MD). In this case, add the following record in “Dombox Domain” DNS.

> _sad.facebook.com => “v=sad1 mailchimp.com instagram.com:r+m -all”

SAD Types

Three kinds of SAD available:

1. Box SAD
2. Local SAD
3. Global SAD

Box SAD

Problem: A system would fail when it expects immediate total cooperation from everybody at once. We cannot expect the websites to support SAD record in our early years. On the other hand, we cannot just assume that the websites gonna use only their “Dombox

Domain" to send mails. For example, Facebook always sends their notification mails from facebookmail.com. If you create a box for "facebook.com", it won't accept those notification mails unless SAD configured.

Solution 1: Let the box learn from its initial users. e.g. 100 Users. We are gonna give unrestricted access to the box for X days for the first X users who create the box. e.g. 30 days.

Example: You created an isolated mailbox for randomdomain.com and you are one of the first 100 Users. For the first 30 days the box gonna work like a Normal Mailbox. i.e. It can accept mails from any domain. The box aggregates and generates a SAD record from those first 100 Users.

Pros: After 100 Users we have enough data for SAD

Cons: Problem with Novice users. There is one more issue. First 100 users can abuse the system by creating duplicate accounts in 3rd party websites. We should have maximum SAD Domains to minimize such abuse. e.g. 10

Solution 2: Collect SAD data from user other mail account mails. Ask the user to import their old mails. So it can be searchable in our system. e.g. @gmail.com, @outlook.com This solution makes sure users won't have any problem with their currently signed up domains.

Solution 3: Purchase the SAD data from data mining companies. Since SAD record contains only non sensitive public data, this is totally ethical.

Message Domain => Array of Envelope Domain. => Total Mails and Total Users for each Envelope Domain.

e.g. example.com => array("mailchimp.com" => "found 573 mails in 33 user accounts", "sendgrid.net" => "found 273 mails in 13 user accounts")

Local SAD

This is the SAD Record added by our company staff for the notable domains.

We should have a threshold for a domain to be considered as a notable domain. e.g. 10 million users

Our staff collect the data from various sources and then define the SAD Record.

This may sound like a tedious process, but it actually is not due to the following reasons.

1. Unlike SPF (which deal with IP addresses), we are dealing with only the “domain names” in SAD. So the data is a stable one since rarely it get changed. Once a SAD record added by our staff, no need to intervene until there is a problem.
2. We can cover most of these notable domains if we process old emails from Gmail, YahooMail etc. So we can ask our users to import their old emails.
3. We can contact these notable sites directly and collect the data from them.
4. All these notable sites, usually have their own mail server setup and do not depend on third party mailing services to send out mails. So they usually use the “reject” policy in DMARC record. Which means there won’t be any SAD Domains for such sites except in rare cases like Facebook. [We can discuss this part in Alignment Layer section]

Global SAD

This is the SAD record defined in the “Dombox Domain” DNS by the domain owner in this path.

> _sad.domboxdomain.com

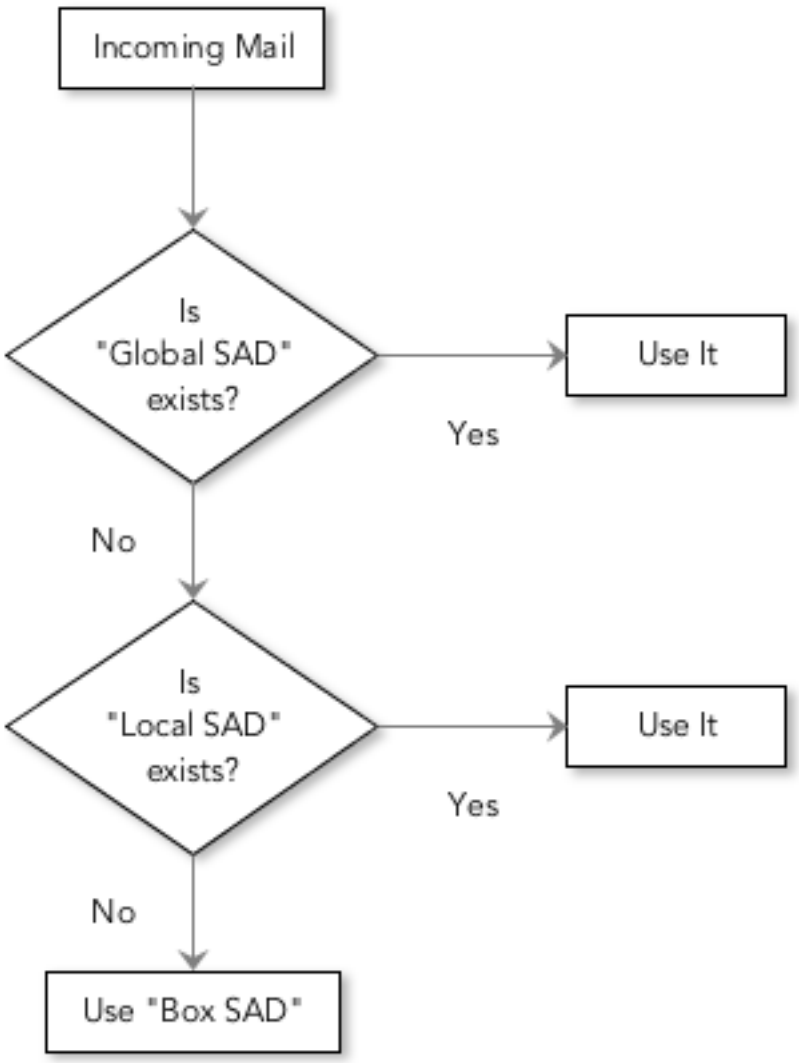


Figure 21: SAD Record Selection

Notes For Bulk Mailers

The SAD record will be checked when you issue RCPT TO command.

When you issue multiple RCPT TO commands (i.e. multiple recipients) make sure they are all related to the same “Dombox Domain” for better results.

To prevent DDoS attacks, we allow up to 10 SAD record failures. The whole session will be terminated with an error message like "Too many SAD Failures" if there are more than 10 SAD record failures.

If the Alias Layer is Fail for a "Dombox Domain", then all consecutive RCPT TO commands related to that "Dombox Domain" will result in Failure too. So if you get a response like "Alias Layer Failure", then either terminate the session or move on to the next "Dombox Domain"

Avoid sending mails to more than 100 different "Dombox Domains" in a single session.

Note: The values 10 and 100 may get changed in the future. So make sure to check our official documentation instead of relying on this document.

Sample SAD Record Query

Note: The SAD record will be fetched from the **Dombox Domain**

Domain	Can be extracted from
Dombox Domain	RCPT TO: <giri123$buyapples.in@domboxmail.com>

Record Path: _sad.domboxdomain.com

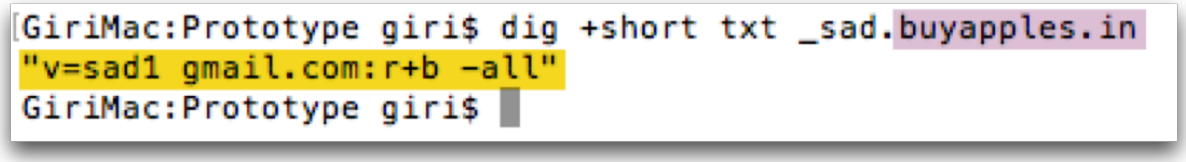


Figure 22: SAD Query

Note: Although we use gmail.com as an example in our screenshot, it is an invalid SAD

domain. {We can discuss about this in a later section}

Authentication Layer

This layer checks whether the mail is digitally signed

Technical Name: DomainKeys Identified Mail (DKIM)

Possible Results: Pass or Neutral or Fail

Pass - Digitally Signed and Signature Verification Passed

Neutral - Digitally not Signed

Fail - Digitally Signed, but Signature Verification Failed

Note: The Signature verification requires a “Public Key”. The public key will be fetched from the **Signature Domain**

This layer consists of four steps.

Step	Done By
Key Generation	Website Owner
Key Deployment	Website Owner
Signing	Sending Server
Verification	Receiving Server

Step 1: Key Generation

Authentication Layer is all about digital signatures.

Digital Signature involves two keys. Private Key and Public Key

The website owner needs to generate these keys.

Note: A real digital signature that involves signing agreements is end to end. However,

we use digital signatures in “Authentication Layer” for message integrity checks in order to prevent email forgery. So organization wide signature is enough for that.

e.g. john@example.com => A real end to end digital signature means, John has his own Private Key and Public Key. Organization wide signature means, only the example.com has Private Key and Public Key

Step 2: Key Deployment

Private Key will be deployed in the server and only used when sending mail (For signing)

Note: Private Key should be kept private always

Public Key will be deployed in the domain DNS. So anyone in the world can access them (For verifying the signature)

e.g. The following is what Facebook has in its DNS

“k=rsa; t=s; h=sha256; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB……..”

The p part is the base64 encoded public key

Hash

Can you identify a bunch of text you typed or photo you have taken or a video you captured or any other digital file for that matter without looking at its contents?

With the help of “Hash” you can

Hash is a unique string that identifies the given file or string.

Hash is a One Way Ticket. Meaning… you can create Hash as long as you have the original message but you cannot create the original message from the hash.

Hash is not a secret value. Hash can be created by anyone as long as they have the original message. The hash value for “SomeRandomString” gonna be the same for you and the person who live in other side of the world.

Hashes are fixed length string. No matter how much data you feed, you always going to get fixed length hash.

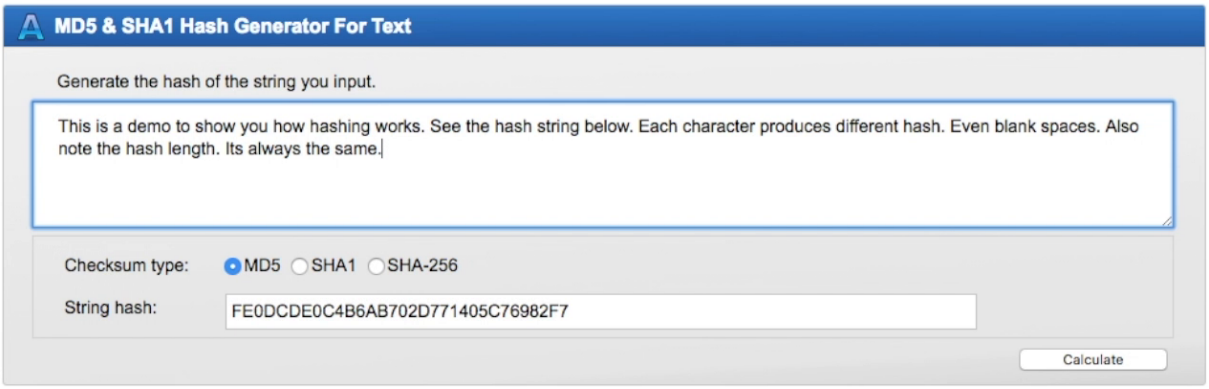


Figure 23: Hash Demo

Hashes are about two rules.

Rule 1: Each Hash must be unique

Rule 2: Ditto Rule 1

When a hashing algorithm produces the same hash for two different strings, then it's called collision. Such algorithms are considered broken and will be discontinued for security reasons. e.g. MD5[62] and SHA1[63] both are vulnerable to collision attacks.

Use Case 1: Passwords => Your passwords are hashed first before storing it in servers

Use Case 2: Storage => For Identifying duplicate content and saving storage space (e.g. File and video hosting websites)

Use Case 3: Anti-Virus => For scanning malicious files. If the file hash in your computer, match a malicious file hash found in your Anti-virus software hash list, then that's a virus file

[62] https://en.wikipedia.org/wiki/MD5#Collision_vulnerabilities
[63] https://shattered.io/

Use Case 4: Integrity => File integrity check after downloading a file from the internet.

Use Case 5: Digital Signatures (See the next few slides to understand how digital signatures work)

Step 3: Signing

Generate Hash from the "Original Message"

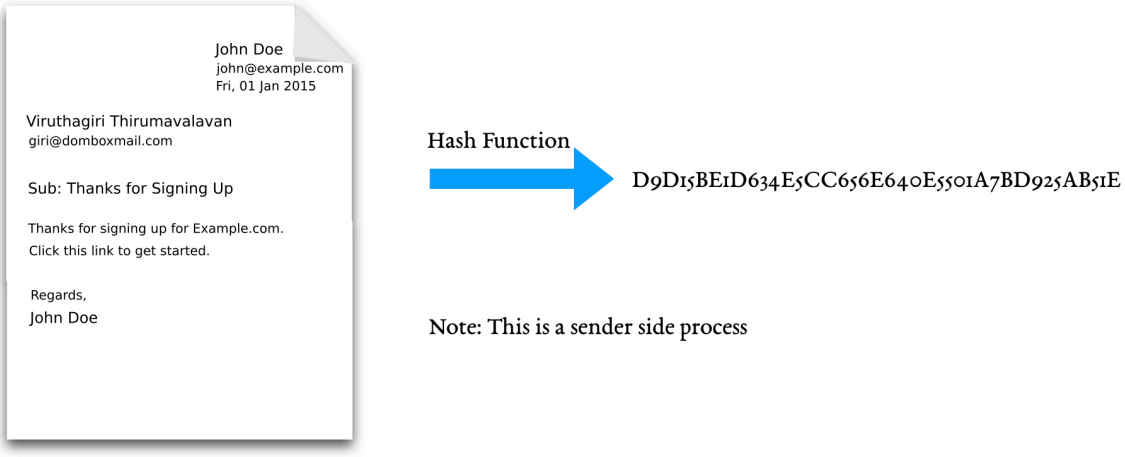


Figure 24: Generate Hash

Encrypt the Hash

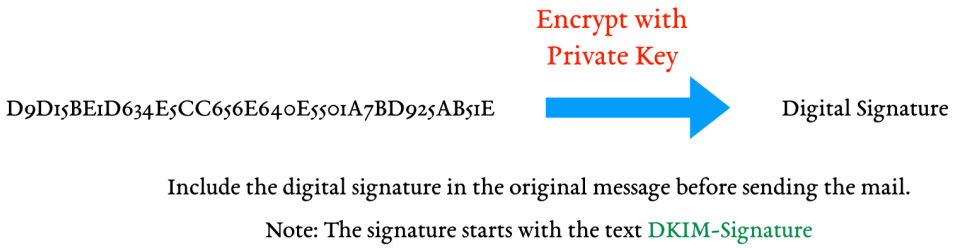


Figure 25: Digital Signature

Step 4: Verification

Generate Hash from the "Received Message"

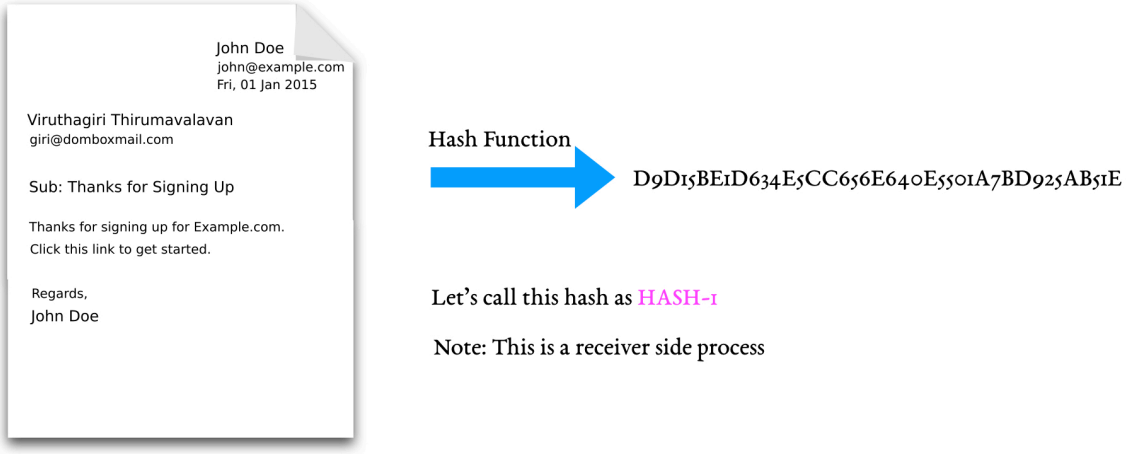


Figure 26: Generate Hash

Decrypt the "Encrypted Hash"

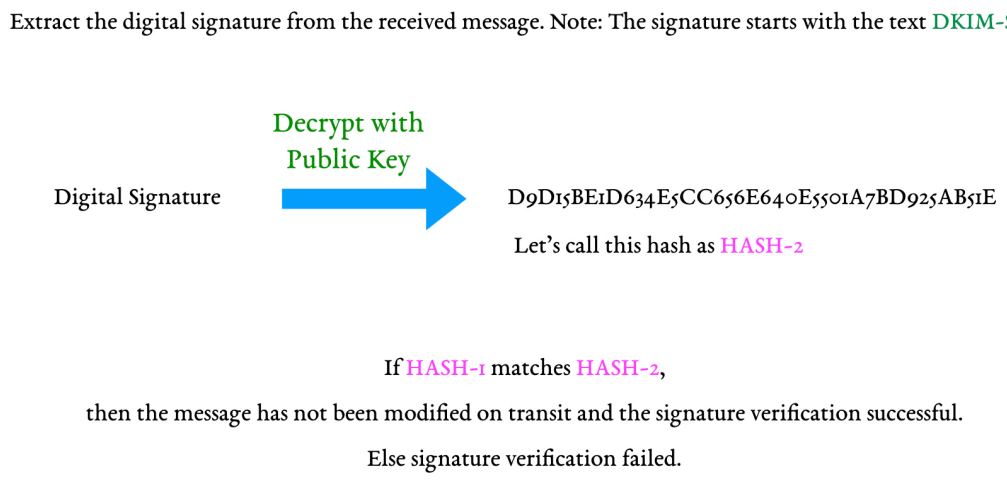


Figure 27: Signature Verification

Sample DKIM Public Key Query

Note: The DKIM public key will be fetched from the **Signature Domain**

Domain	Can be extracted from
Signature Domain	*DKIM-Signature: a=rsa-sha1; q=dns; s=s1024-2013-q3; d=**facebookmail.com**; .....*

Sample DKIM Signature found in the received mail

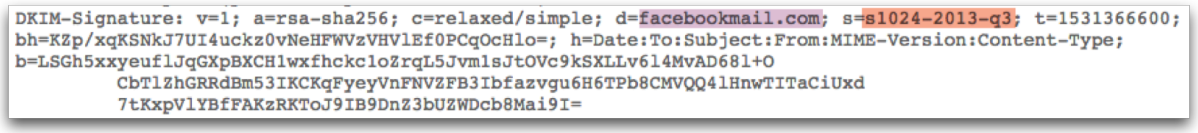


Figure 28: Sample DKIM-Signature

"b" part is the signature we have to decrypt using the fetched public key.

Record Path: selector._domainkey.signaturedomain.com

Fetch DKIM Public Key

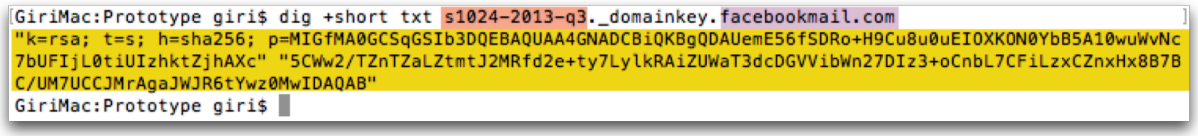


Figure 29: DKIM Query

Alignment Layer

Checks whether the domains are aligned

Technical Name: Domain-based Message Authentication, Reporting and Conformance (DMARC)

Possible Results: Pass or Neutral or Fail

Pass - Domains are aligned

Neutral - Domains are not aligned, but the "Message Domain" either has "No Objection" or no valid DMARC record found in the "Message Domain"

Fail - Domains are not aligned and the "Message Domain" has "Objection"

Note: The DMARC record will be fetched from the **Message Domain**

"You can send mails for the domain you don't own". That's what the third-party newsletter services like mailchimp doing right?

So tell us this. What's stopping the spammers from misusing your domain? If you own a domain called abcd.com, what's stopping the spammers from sending "Viagra" mails from an email address like no-reply@abcd.com? This is called "Email Spoofing"

Many spammers use the spoofing method to send Phishing mails.

Companies like PayPal had been a major victim of Phishing mails in the past.

Companies like PayPal, your banking website etc. can't afford when spammers misuse their domain.

Hence DMARC came to the rescue.

This layer protects the "Message Domain". This Layer is all about 3 domains too.

In Alias Layer, Dombox Domain (Primary Subject) compares itself with "Envelope Domain" and "Message Domain". Purpose: To "Allow" third party domains.

Just like that, In Alignment Layer Message Domain (Primary Subject) compares itself with "Envelope Domain" and "Signature Domain". Purpose: To "Deny" third party domains.

When all three domains look exactly the same, then its already aligned. We just accept the mail

But if there is even a small change (e.g. subdomain) or completely different domains used, then we need to ask the "Message Domain" about how we should treat the mail?

If there is no DMARC record found in the "Message Domain" DNS, then the ball is in our court. So we use our version of the book to play the game

If a DMARC record found in the "Message Domain" DNS, then we should treat the mail as they say. This is called DMARC policy

The policy can be one of the three things. None, Quarantine or Reject

Policy	Meaning
None	Do whatever you want
Quarantine	Put in the spam folder
Reject	Reject the mail immediately

The following DMARC record is what PayPal has in its DNS at this location => _dmarc.paypal.com

“v=DMARC1; p=reject; rua=mailto:d@rua.agari.com; ruf=mailto:d@ruf.agari.com”

You know.. We actually wanted to call this layer “Objection Layer”

This is because this layer is all about asking a question to the “Message Domain”.

Hey “Message Domain”, The domains are not aligned. But our server is going to accept this mail. Do you have any objection?

The response will be one of the following.

Policy	Meaning	Result
None	I have no objection	No Objection
Quarantine	Yes I have an objection, Put in the spam folder	Objection
Reject	Yes I have an objection, Reject the mail immediately	Objection
No Record	I don’t know what you are talking about	No Objection

From the last table, we can come to a conclusion, a message domain can have either objection or no objection.

We can mark this layer as “Pass” when domains are aligned

We can mark this layer as “Fail” when the “Message Domain” has “Objection”. i.e. Quarantine or Reject

We can mark this layer as “Neutral” when the “Message Domain” has “No Objection”. i.e. None or No Record

However, we need a small change for the incoming mails to the boxes found in “Domboxes” group.

In Domboxes, We should mark this layer as “Pass” when the “Message Domain” has “No Objection”. i.e. None or No Record

As of 2018, 332 million[64] domains are registered so far.

In “Mailboxes” case, receiving mails is like opening a can of worms. The DMARC is the “Iron Grip”. So it gives us clarity. i.e. 332 million domains can send mails to the mailbox

In “Domboxes” case, only the “Dombox Domain” and its SAD Domains can send mails to the Dombox. So we are talking about only a handful of domains here

But still, we need to make sure that the Message Domain has no Objection, before accepting the mail.

For example, if a domain owner configured SAD record like this “v=sad1 paypal.com:r+m -all”, then we shouldn’t just take his word for it

So if there is no DMARC record found in the “Message Domain”, then we take the “Dombox Domain” owner’s word for it. Because we are hoping they won’t ruin their domain reputation by whitelisting domains in their SAD record for email spoofing.

Our point is that “Alignment Layer” can be “Neutral” in “Mailboxes”. But can’t be in “Domboxes”. Because if there is no DMARC record found or None value configured then we just accept the mail by marking the result as “Pass”

Sample DMARC Record Query

Note: The DMARC record will be fetched from the **Message Domain**

[64] https://blog.verisign.com/domain-names/verisign-q4-2017-domain-name-industry-brief-internet-grows-332-4-million-domain-name-registrations-fourth-quarter-2017/

Domain	Can be extracted from
Message Domain	*From: Support <support@paypal.com>*

Record Path: _dmarc.messagedomain.com

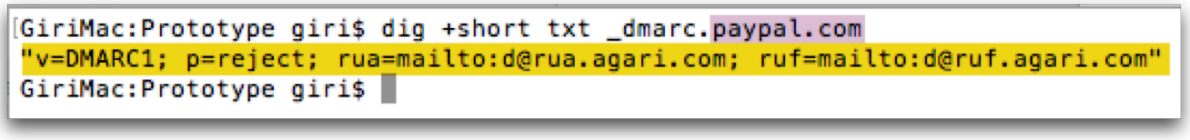


Figure 30: DMARC Query

Possible Results

Layer	Pass	Neutral	Fail
Encryption Layer	Yes	No	Yes
Authorization Layer	Yes	Yes	Yes
Alias Layer	Yes	No	No
Authentication Layer	Yes	Yes	Yes
Alignment Layer	Yes	Yes*	Yes

* Not Applicable for the boxes found in “Domboxes”

Layer Purpose

Each layer serves a different purpose

Layer	Description
Encryption Layer	Establishes Secure Communication.
Authorization Layer	Prevents “Envelope Domain” Spoofing.
Alias Layer	Allows non “Dombox Domain” to send mails to the Dombox.
Authentication Layer	Proves Mail Genuinity.
Alignment Layer	Prevents “Message Domain” Spoofing.

SPF vs DKIM vs DMARC

All these three mechanisms are widely used to combat **email spoofing**.

There is a misconception that SPF, DKIM and DMARC helps the receiver to combat spam. That’s not true. All three mechanisms are open standards. So any domain owner can deploy them since they are free. That means a spammer can deploy them too.

If a domain get blacklisted, then the spammer would go for new domain. You can register domains for free these days. Freenom[65] offers free domains[66] for the following extensions. .tk, .ml, .ga, .cf, .gq

When a domain owner configures those three mechanisms in their domain, then scammers cannot misuse that domain.

Mechanism	Type
SPF	Direct
DKIM	Indirect
DMARC	Complimentary

[65] https://www.freenom.com/
[66] https://www.freenom.com/en/freeandpaiddomains.html

SPF would work only for **direct** flow.

e.g. accounts@paypal.com sends an email to johndoe@gmail.com. PayPal whitelisted the following IP addresses in their SPF record. {100.100.100.100, 200.200.200.200}. PayPal sends that mail from the IP address 100.100.100.100. gmail.com verifies SPF and it is a pass.

But what happens when johndoe@gmail.com enabled "mail forwarding" and asks gmail to forward his incoming mails to johndoe@yahoo.com? When we mean "mail forwarding" we are talking about the "server forwarding" here, not the "Forward" option you see in the email clients/apps.

When a mail gets forwarded from gmail.com to yahoo.com server, the sender IP will be the gmail.com IP address. Not paypal.com IP address. So the SPF would fail.

Mailing list / Discussion list heavily relies on "mail forwarding". So there is a need for "Indirect" mechanism. That's where DKIM comes to play.

SPF deals with "Envelope Part". DKIM deals with the "Message Part". DMARC deals with *SPF and DKIM results*

In other words, DMARC alone cannot able to combat email spoofing. It needs to rely on at least SPF or DKIM in order to work. The more the merrier here. Meaning, you should always configure both SPF and DKIM before deploying DMARC for better coverage. However, DMARC can work with only one method too.

Chapter 7: Mail Score

Our "Layers" component contains 5 layers.. right?

Encryption Layer, Authorization Layer, Alias Layer, Authentication Layer, Alignment Layer

One point will be given for each layer if the result is "Pass"

We will be displaying the score in each mail. If you click the score, you can view detailed info

Keep in mind, the score can be from 1 to 5 {Note: Alias Layer will always have the “Pass” value. So the minimum possible score is one.}

A score of 2 means, 2 layers passed. But that doesn’t mean 3 layers failed. Because these three layers can also be “Neutral”

When the score is “5”, a “Green Checkmark” will be displayed instead of the score “5”

If you see the score in “Green Circle”, that means the layer results contains only “Pass” and “Neutral” values

If at least one layer result is “Fail”, then the score will be shown in “Red Circle”. Be sure to check the info by clicking the score

By giving a score to each mail, we bring “transparency” to the user. Now users can question the website owners why they are not supporting those layers

For example, if your banking website doesn’t support “Encryption Layer”, then you have every right to question them

If you are a website owner, most likely you want your users to see the “Green Checkmark”. So we are also encouraging the website owners to support all 5 layers

Note: Mail Score is applicable only for “Incoming” mails

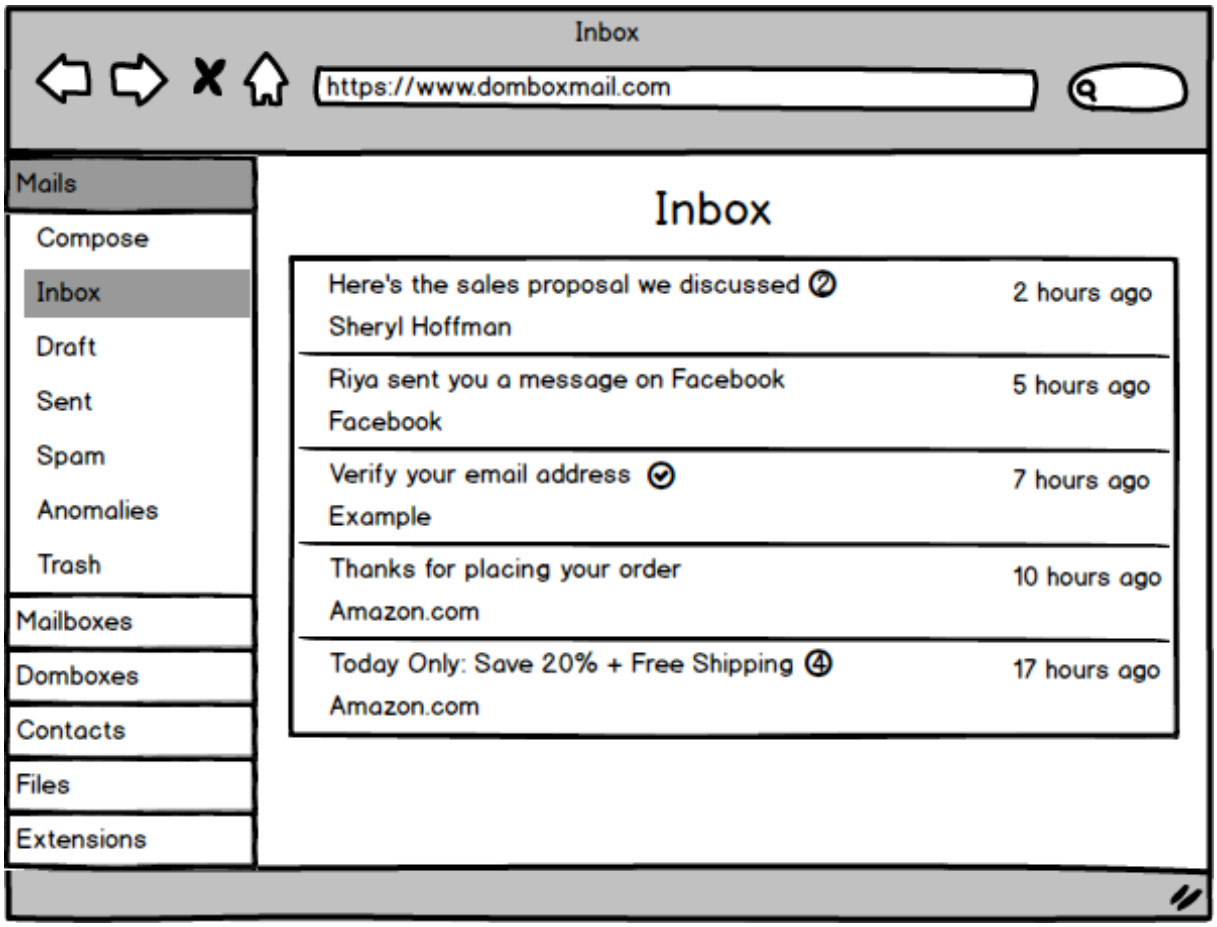


Figure 31: Mail score - List View

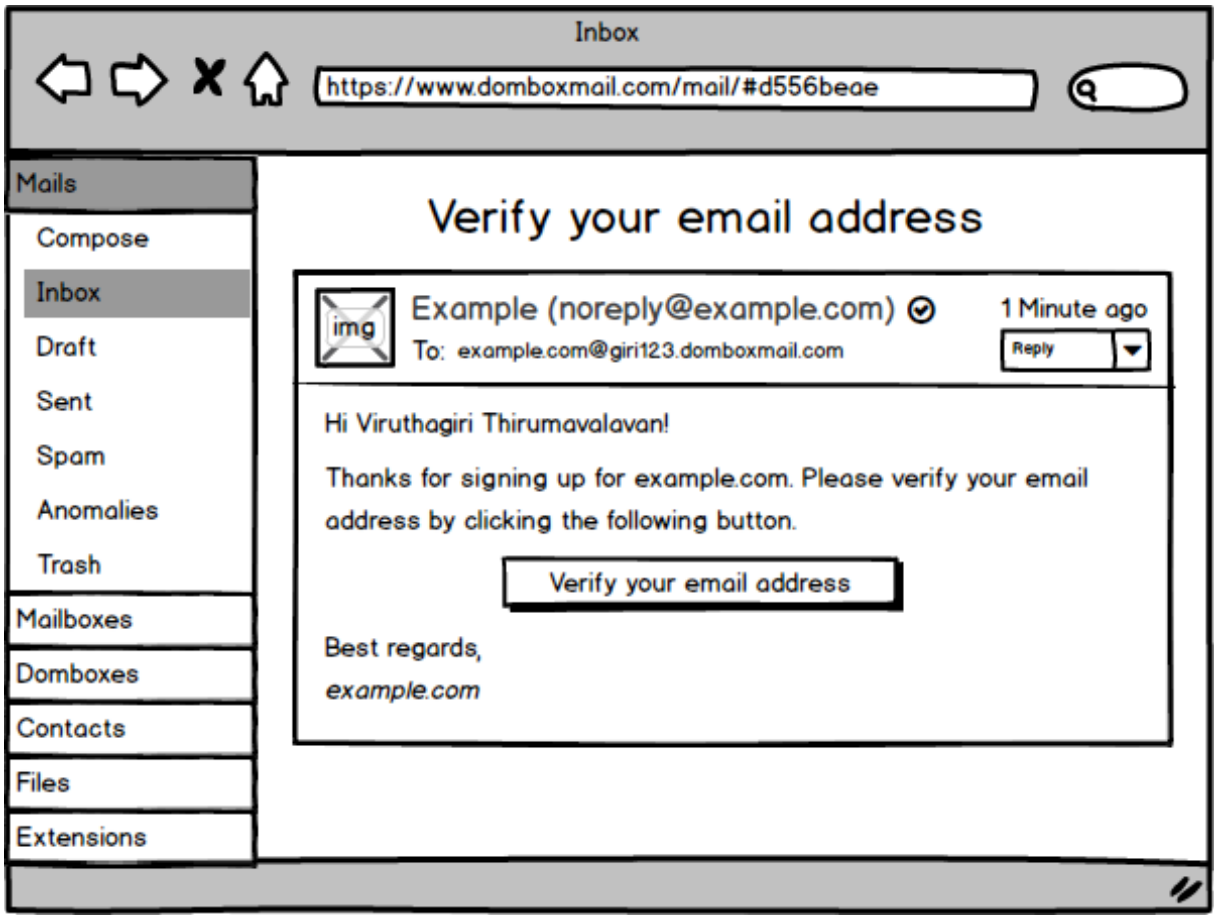


Figure 32: Mail score - Single View

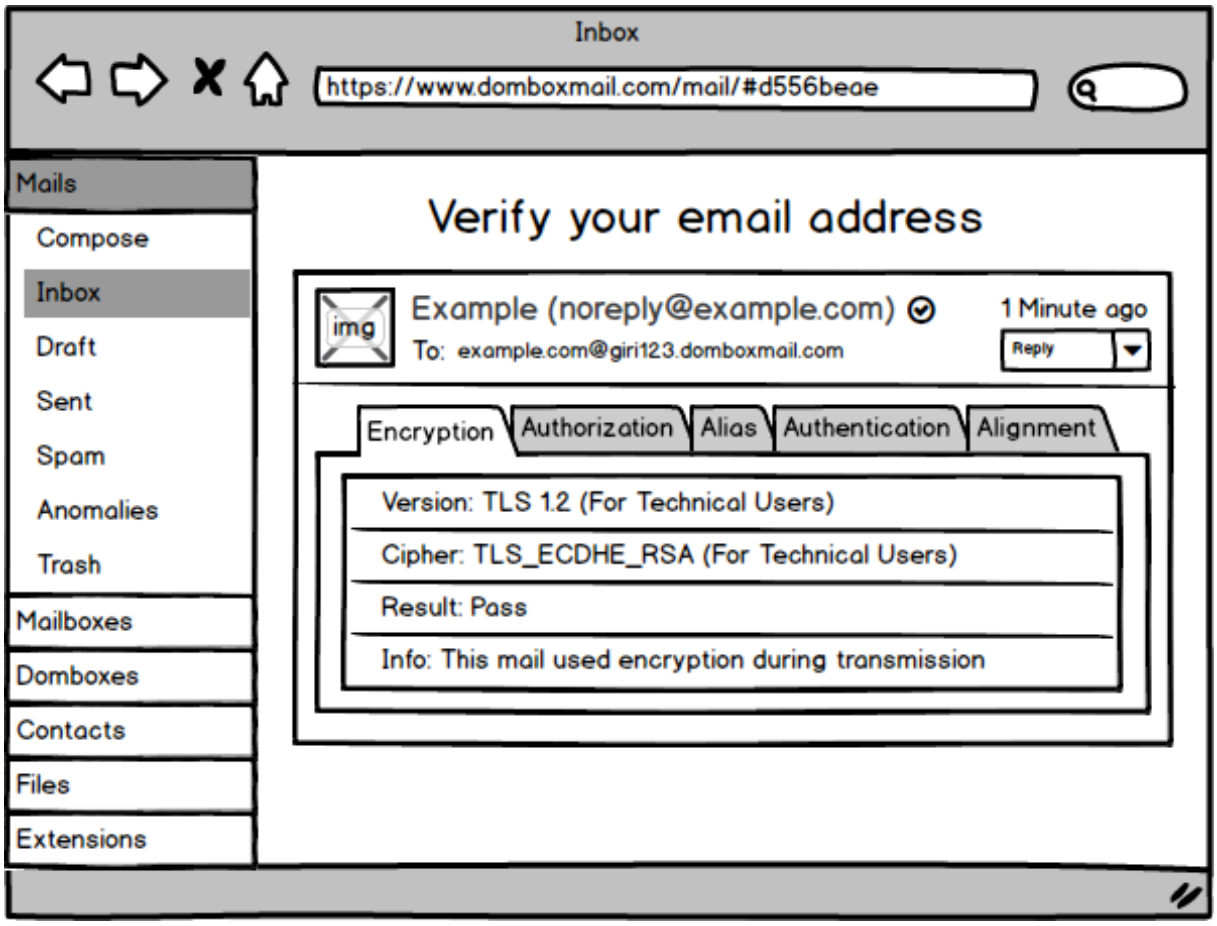


Figure 33: Mail score - Encryption Layer

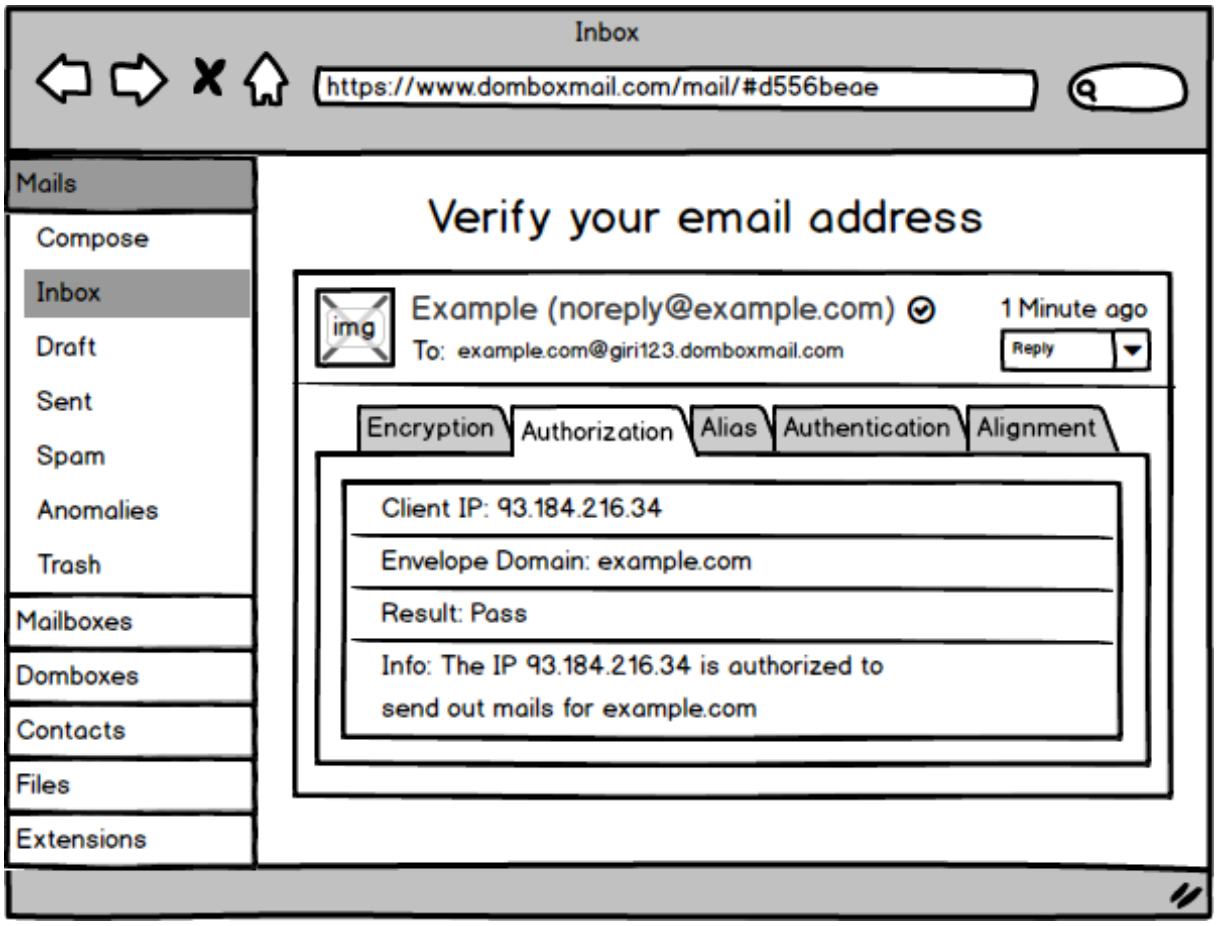


Figure 34: Mail score - Authorization Layer

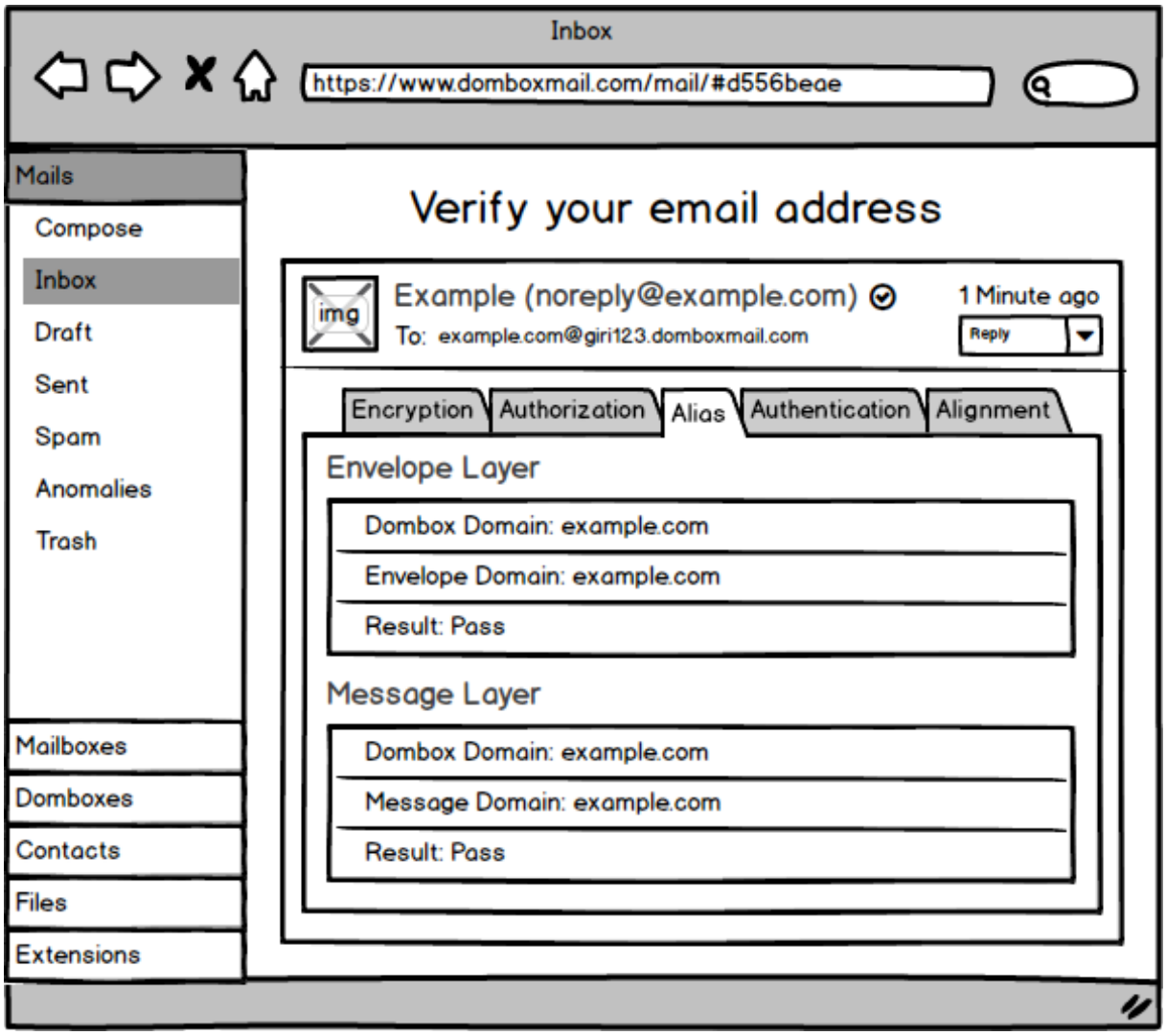


Figure 35: Mail score - Alias Layer

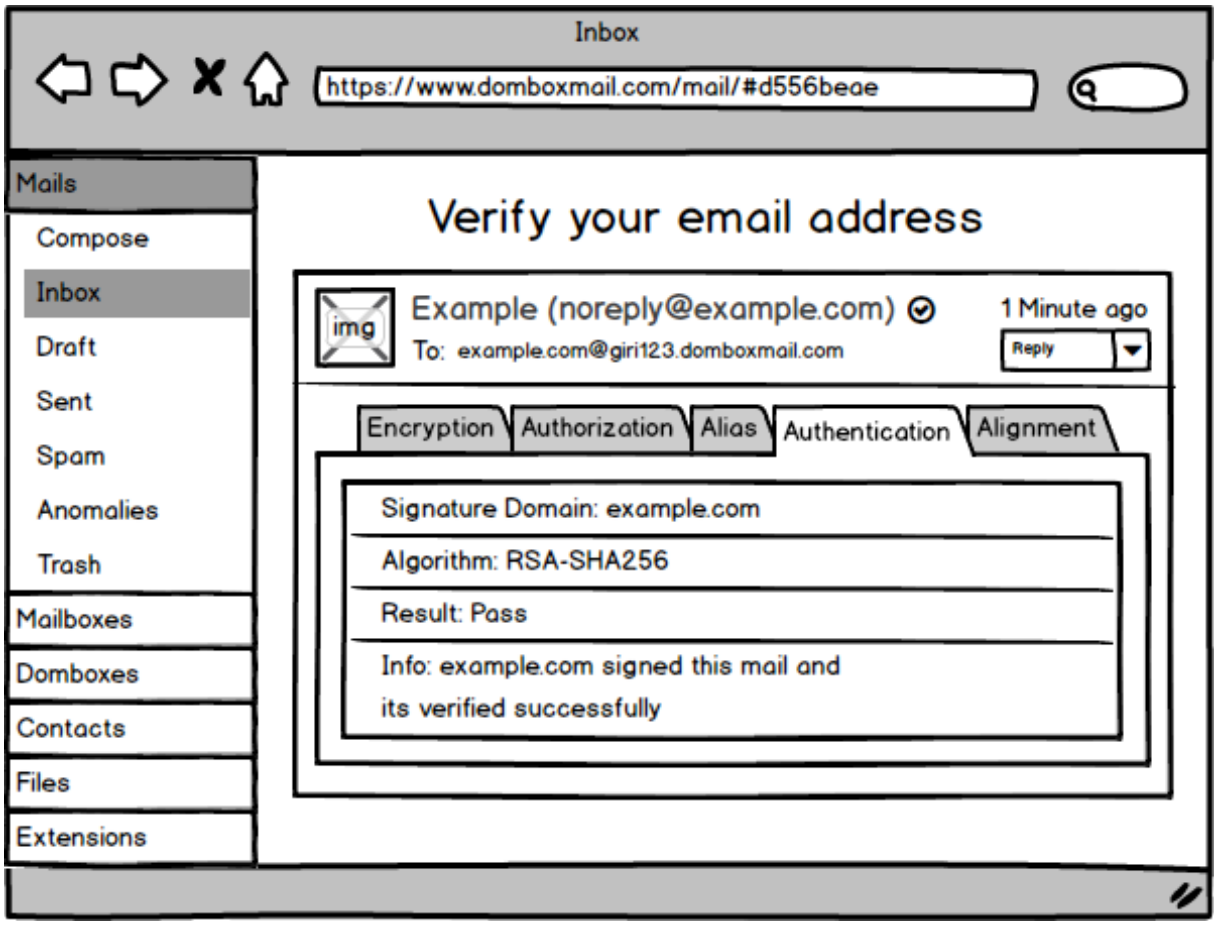


Figure 36: Mail score - Authentication Layer

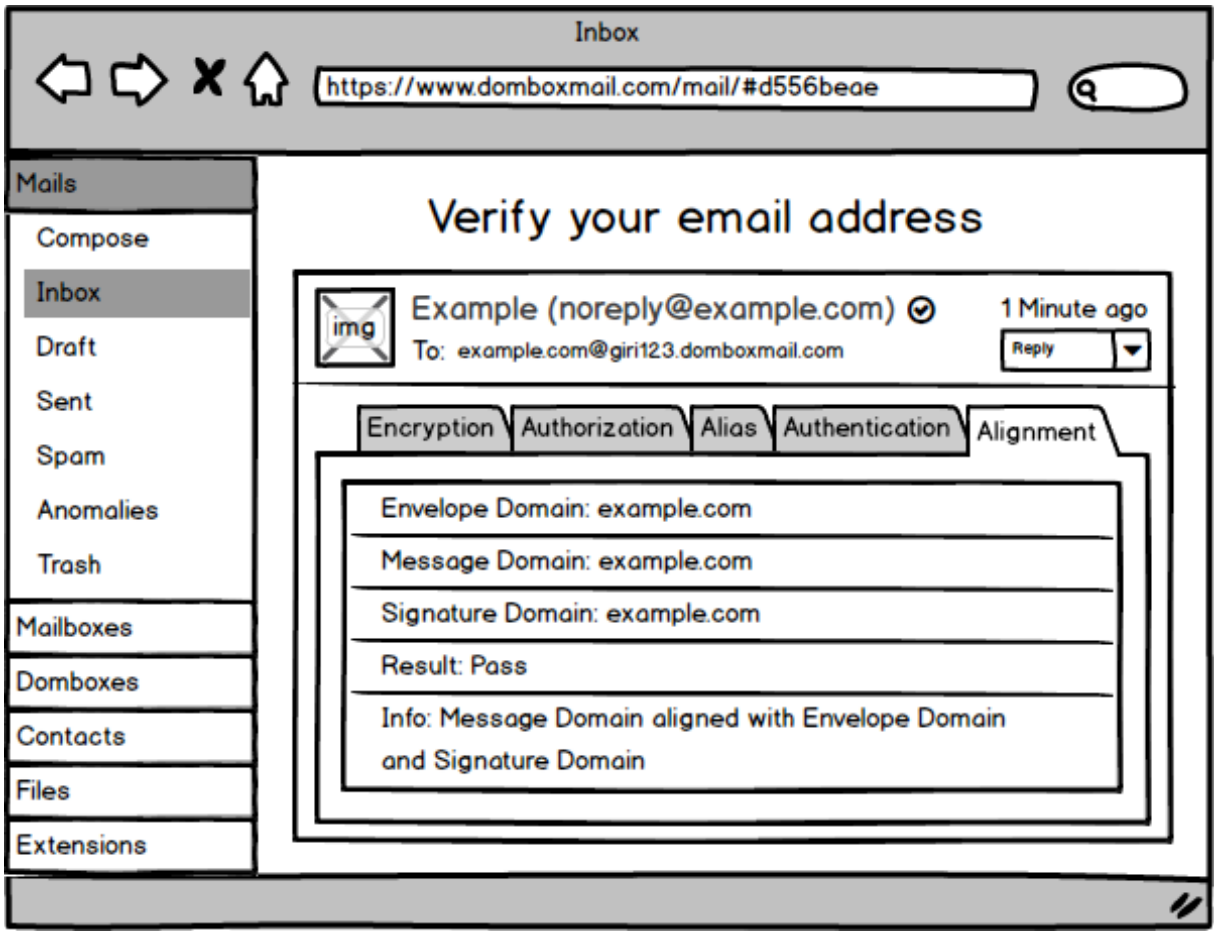
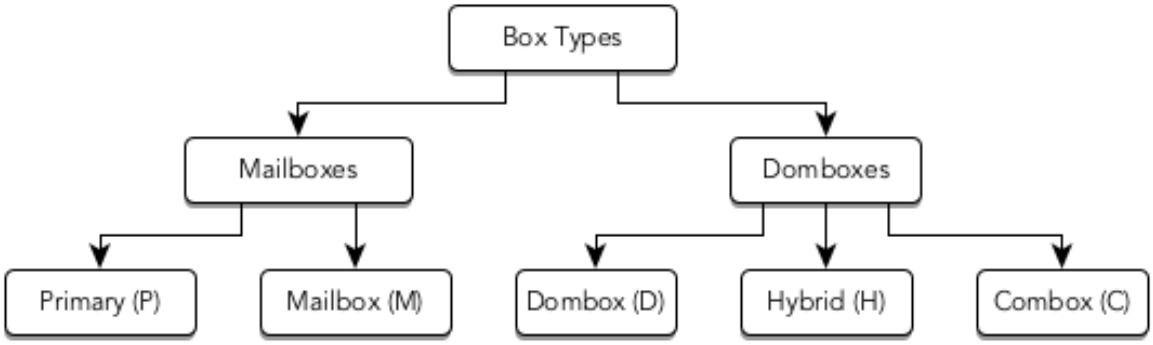


Figure 37: Mail score - Alignment Layer

Chapter 8: Box Types



Our system contains 5 type of boxes

Box Type	Box Group	Purpose
Primary (P)	Mailboxes	To have a “Normal Mailbox” that works exactly like Gmail
Mailbox (M)	Mailboxes	To use as a 3rd party Mail Client. e.g. @gmail.com & To use as a 3rd party mail server. e.g. @yourcompany.com
Dombox (D)	Domboxes	To let consumers have control over the “Isolated Mailbox”
Hybrid (H)	Domboxes	To provide “One-Click” newsletter subscription service
Combox (C)	Domboxes	To let businesses have control over the “Isolated Mailbox”

Must Pass Layers

	Primary (P)	Mailbox (M)	Dombox (D)	Hybrid (H)	Combox (C)
Encryption Layer	-	-	-	Must Pass	Must Pass

	Primary (P)	Mailbox (M)	Dombox (D)	Hybrid (H)	Combox (C)
Authorization Layer	-	-	-	Must Pass	Must Pass
Alias Layer	-	-	Must Pass	Must Pass	Must Pass
Authentication Layer	-	-	-	Must Pass	Must Pass
Alignment Layer	-	-	-	Must Pass	Must Pass

Box Features

Boxes come with the following features.

Feature	Description
Make Offline	When a box is offline, it can't able to accept any mails
Delete	When a box gets deleted, only the box mail address will be lost. But the mails can still be browsed via "Unified Mails" page. The mails can be recovered if you recreate the box. And yes, a deleted box can't able to accept any new mails.
Format	Bulk deletes all the mails found in a particular box. Applicable only for Domboxes. {Normal Mailboxes usually contains Conversational Mails which are very important. So Format option not available in Normal Mailboxes} To completely delete the box along with its mails, you must "format" the box first and then use the "delete" option.
Mute	Prevents annoying mail notifications. Mail will be accepted but you won't be notified when a box is "Muted".
Subscribe	When a user is "Subscribed" to the box, the user is voluntarily asking the site to send newsletters / promotional mails. {Refer Chapter 12: Telescribe for more info}

Feature	Description
Unsubscribe	This option helps you with the unsubscription nightmare. When a user is “Unsubscribed” to the box, the user is asking the site, not to send any newsletters / promotional mails. When the box status is “Unsubscribed” and our system find any new mails with “List-Unsubscribe” header and/or “Unsubscribe” link at the mail footer, then we automatically try to unsubscribe on behalf of the user and then instantly move the mail to the “Trash” folder. If a domain sends Promotional mails without “Unsubscribe” link, then they are breaking the laws.

Inbox

Inbox can be classified into two types.

1. Global Inbox
2. Local Inbox

Global Inbox

“Global Inbox” is also known as “Master Inbox”

This is equivalent to the “inbox” found in other services. “Global Inbox” contains aggregated mails from all 5 box types. So the mails are “Unified” here.

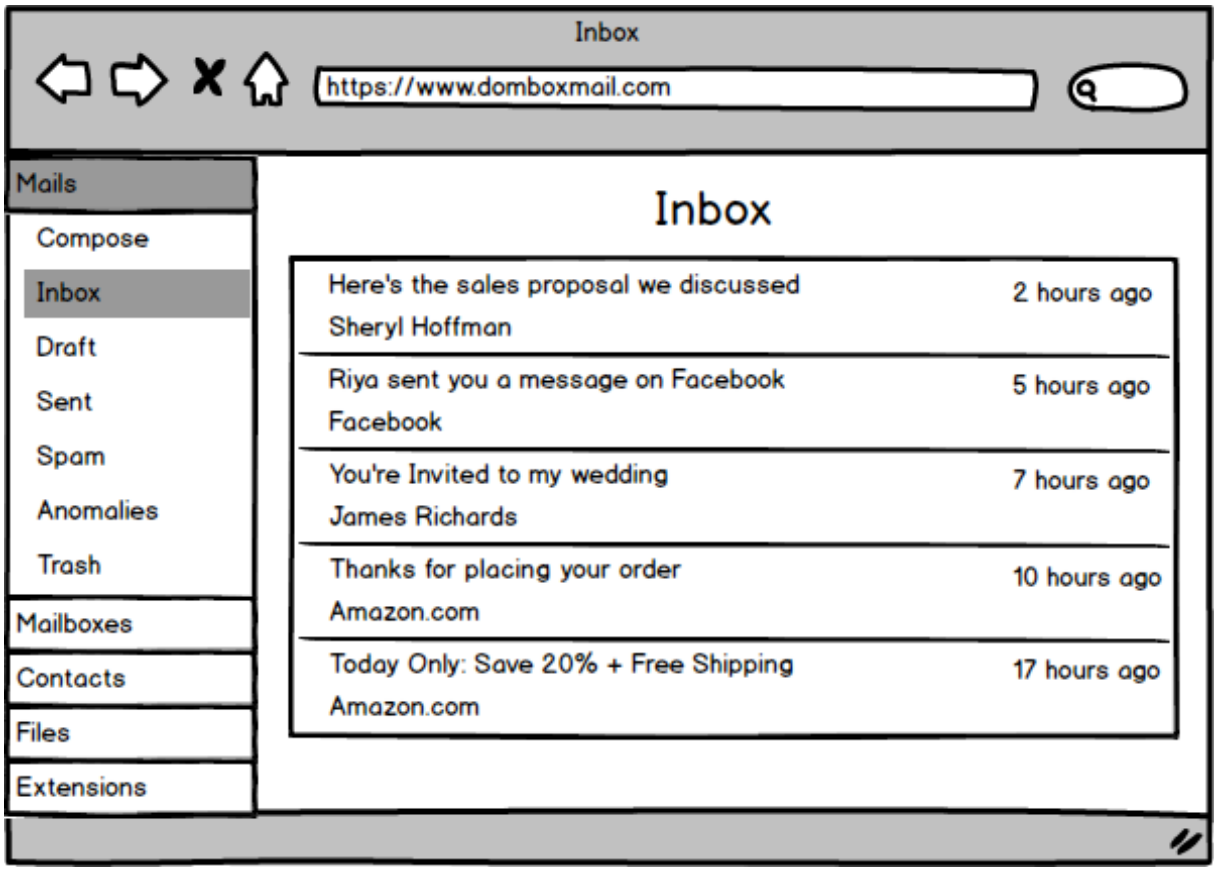


Figure 38: Global Inbox

Local Inbox

This is the inbox found in the individual box. In “Local Inbox” you can browse only that particular box mails.

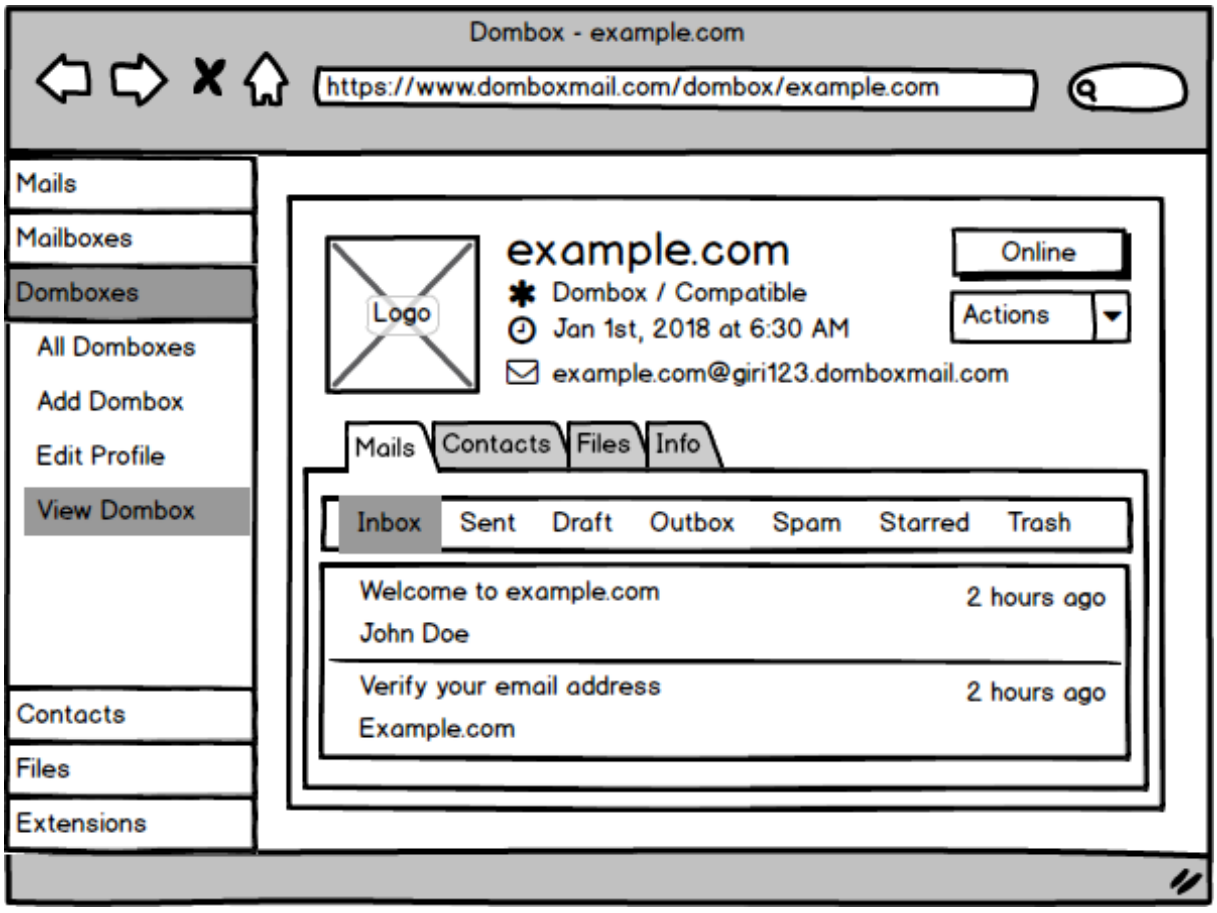


Figure 39: Local Inbox

Box Type: Primary (P)

You can have only one box of this type. Whereas in other box types you can have unlimited boxes. This "only one box" is called "Primary" box.

In our mail service, the "Primary" box is equivalent to your @gmail address. But you are recommended to use this box only for real conversational mails.

Note: We recommend that. Not mandate that. i.e. If you are not planning to use our "Domboxes" feature, then you are welcome to use your Primary box for all type of mails.

This is the box type you get when you signup for our mail service.

How to get this box? Via signup form

Must Pass Layers: None.

Note: Although there is no requirement for "Pass" in this box type, that doesn't mean mail will be accepted when all layers are failed.

Figure 40: Primary Email Address

Box Type: Mailbox (M)

These are additional "Normal Mailboxes". This box type requires a nominal fee. For most users, there won't be a need for this box type. Only the "Primary" box is enough.

A “box” found in Mailboxes group is called “Mailbox”. The term “Mailbox” always refers to any box found in “Mailboxes” group.

Since Primary (P) is also a box type found under mailboxes group, we can call it a Mailbox

Since the term “Mailbox” already refers to any box found in the Mailboxes Group, we use the letter M in parentheses to indicate “Mailbox Box Type”.

In other words, “Mailbox” refers to ANY Box found in “Mailboxes” Group. But “Mailbox (M)” refers to the Box Type found in “Mailboxes” Group.

This box type can behave in two ways.

1. As a Mail Server
2. As a Mail Client

How to get this box? Activate our “Mailboxes” extension and then use the “Add Mailbox” link

Must Pass Layers: None.

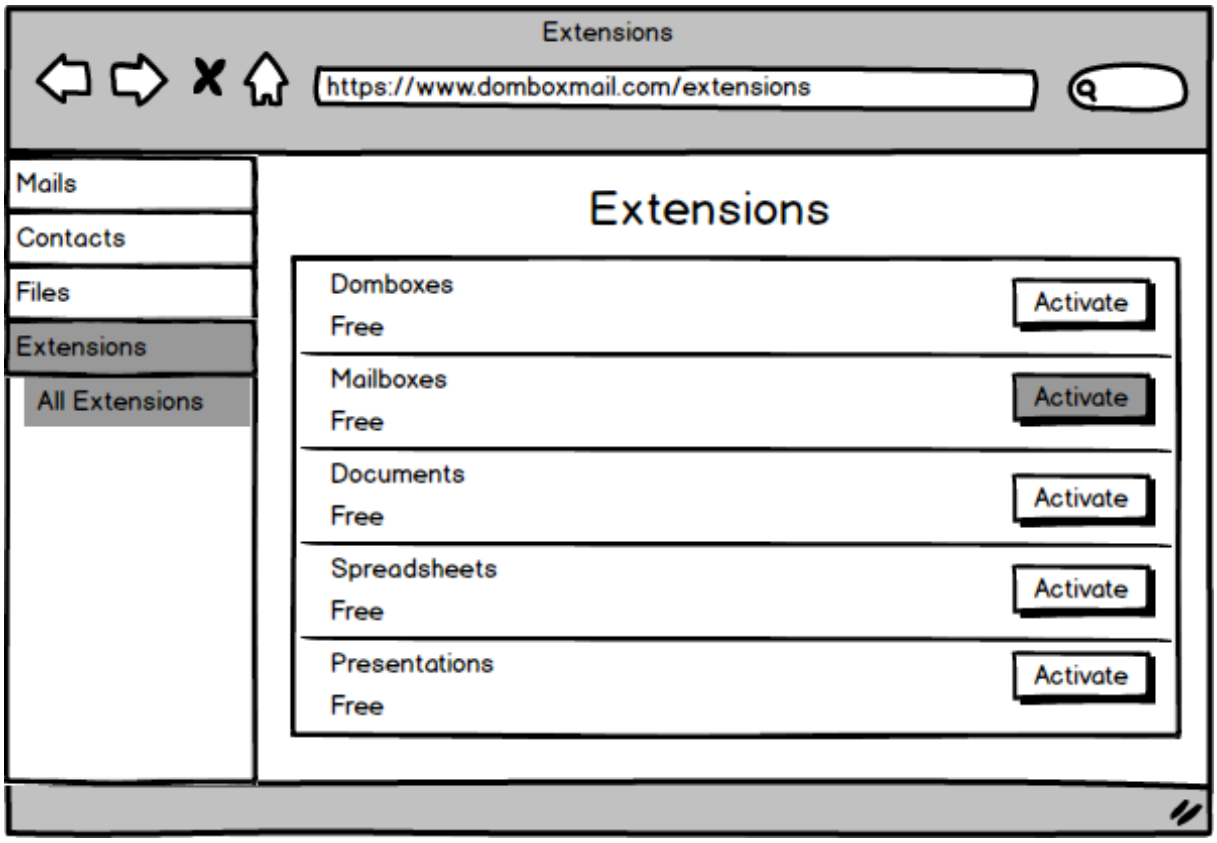


Figure 41: Mailboxes Extension Activation

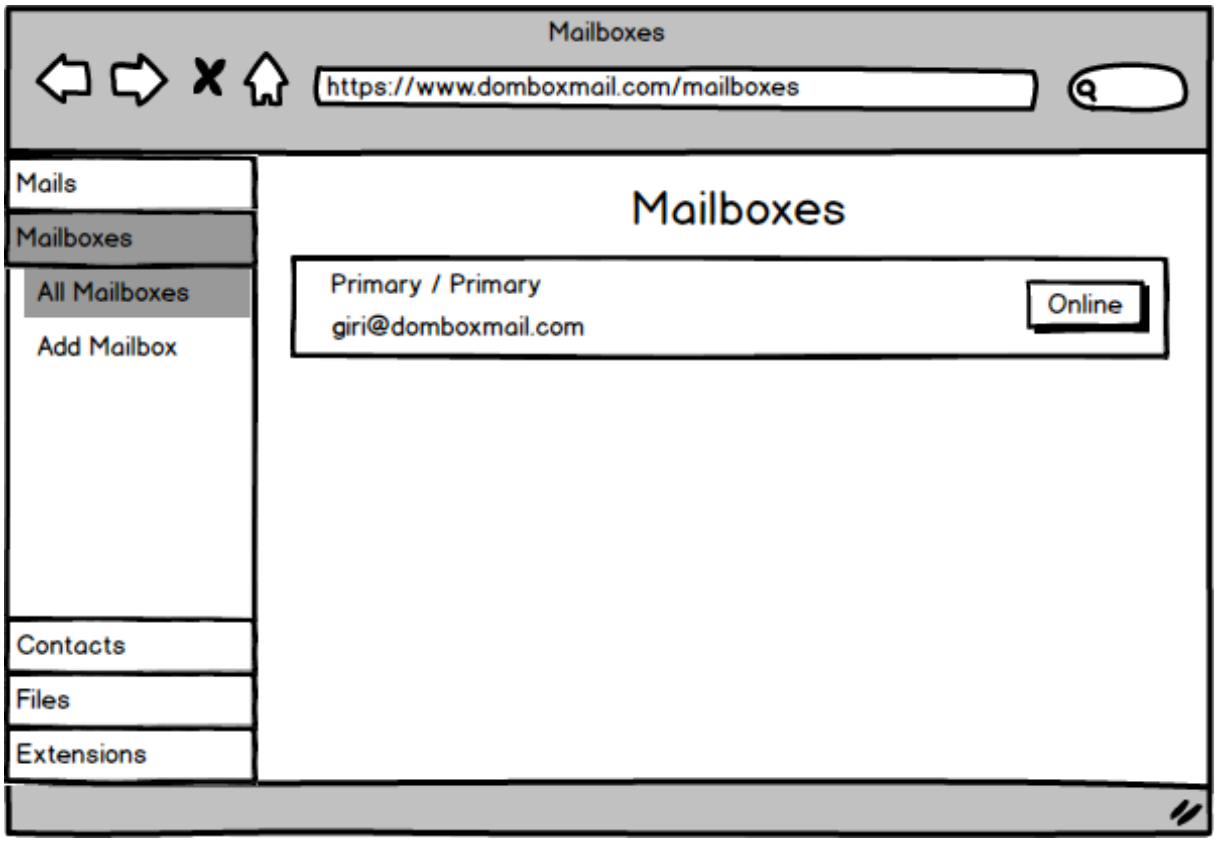


Figure 42: View Mailboxes

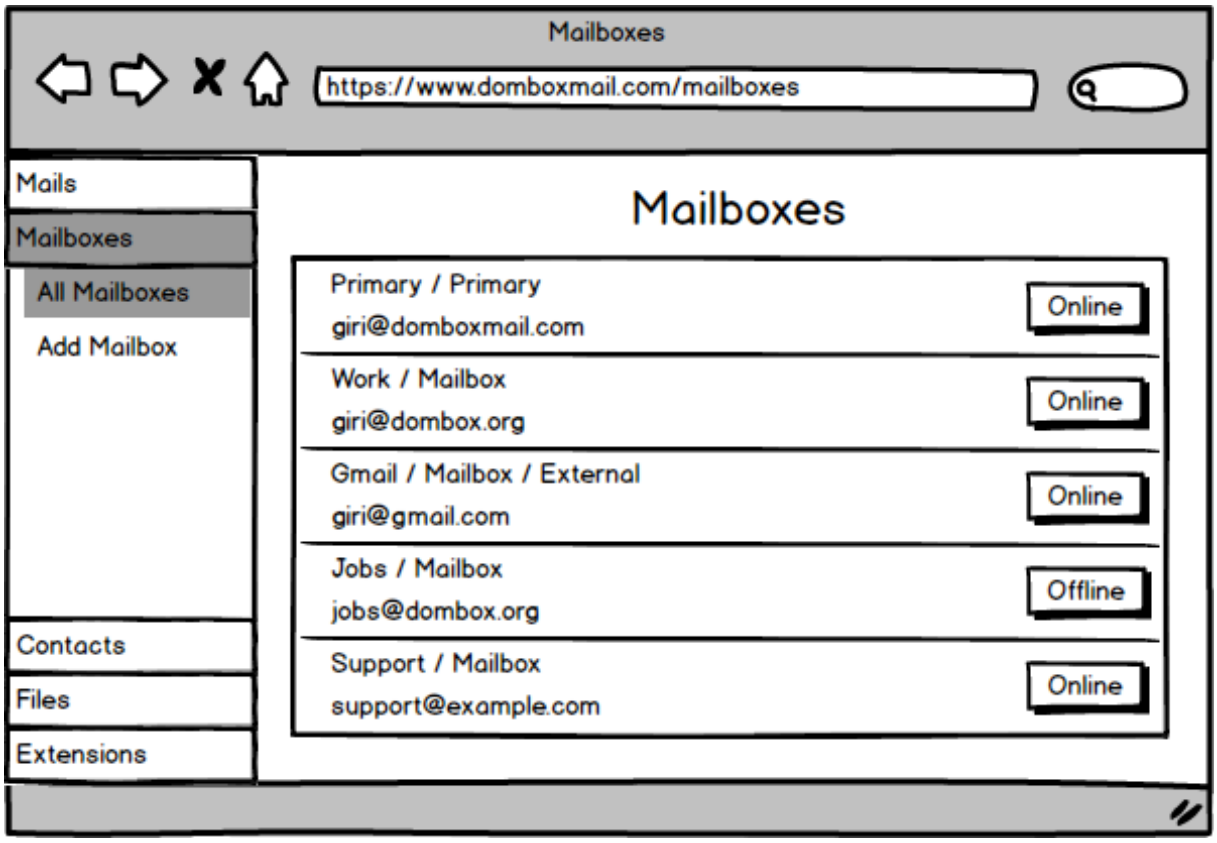


Figure 43: Multiple Mailboxes

As a Mail Server

This is similar to Google's business mail service. You can have mailbox address like @your-domain.com

Keep in mind, you must be a domain owner and you must have access to your domain DNS.

You have to verify your domain first and then add MX records like mx1.domboxmail.net, mx2.domboxmail.net and mx3.domboxmail.net in your DNS

In this case, our mail service act as a "Mail Server".

As a Mail Client

This works similar to “Mozilla Thunderbird” or a mail client found in your mobile.

Keep in mind, you need to already have an Email Account and then add that account here as a “Mailbox (M)” box type.

Is this really necessary? The answer is “Yes”. It’s actually for “Graceful Degradation”

People won’t suddenly switch to another mail service even if you provide world-class service. There are plenty of variables to consider.

You have been using your @gmail.com account for 10 years, would you suddenly jump ship to another service?

But “Customer Acquisition” is a time-sensitive thing. If we wait for them to change their mind, we may have to wait forever.

So we are gonna let them add ONE third party mail account for free. It can be @gmail.com, @yahoomail.com, @outlook.com or even @yourcompany.com

As long as your original mail server support protocols like POP3 and Mail Forwarding, you are good to go.

We will be using protocols like POP3, IMAP, OAuth for fetching the initial mails and then the “mail forwarding” option for the new mails.

This let them gradually degrade their old mail account. For example, if they had signed up for twitter.com with their old @gmail.com address, they can create a “Dombox” now for twitter.com and then update the email address in their twitter account settings page.

That way they can still use @gmail.com in our mail service, but offload the Transactional and Promotional Mails to the Isolated Mailboxes.

Chapter 9: Dombox

We cannot expect every website in the world to support all our 5 layers.

So for Dombox (D) box type, only the “Alias Layer” must be passed. If all other four layer fails then most likely we will reject the mail. But if most of them are “Neutral”, then we may accept the mail.

Let’s say we accept mails even when “Alias Layer” result is “Fail”. This means we are accepting mails from every domain on the Internet. The “Alias Layer” is what makes the Dombox special. Without it, “Dombox” will be equivalent to the “Mailbox” since it’s accepting mail from anyone

Since we are allowing unlimited “Domboxes”, without “Alias Layer”, the users can run their own version of mail service inside their account.

So for Dombox (D) box type “Alias Layer” must be passed for accepting the mail.

Dombox (D) box type has the options “Delete” and “Make Offline”. If somehow a spammer sends you spam mails to the Dombox (D), that means that domain is vulnerable to “email spoofing”. So you have the following options.

1. Ask the spammer politely not to spam you
2. Contact the website owner and demand them to configure “email spoofing” prevention mechanisms like SPF, DKIM and DMARC.
3. Delete the box and move on (This is why we gave you those privileges right?)

To create a Dombox, you need to activate the “Domboxes” extension first.

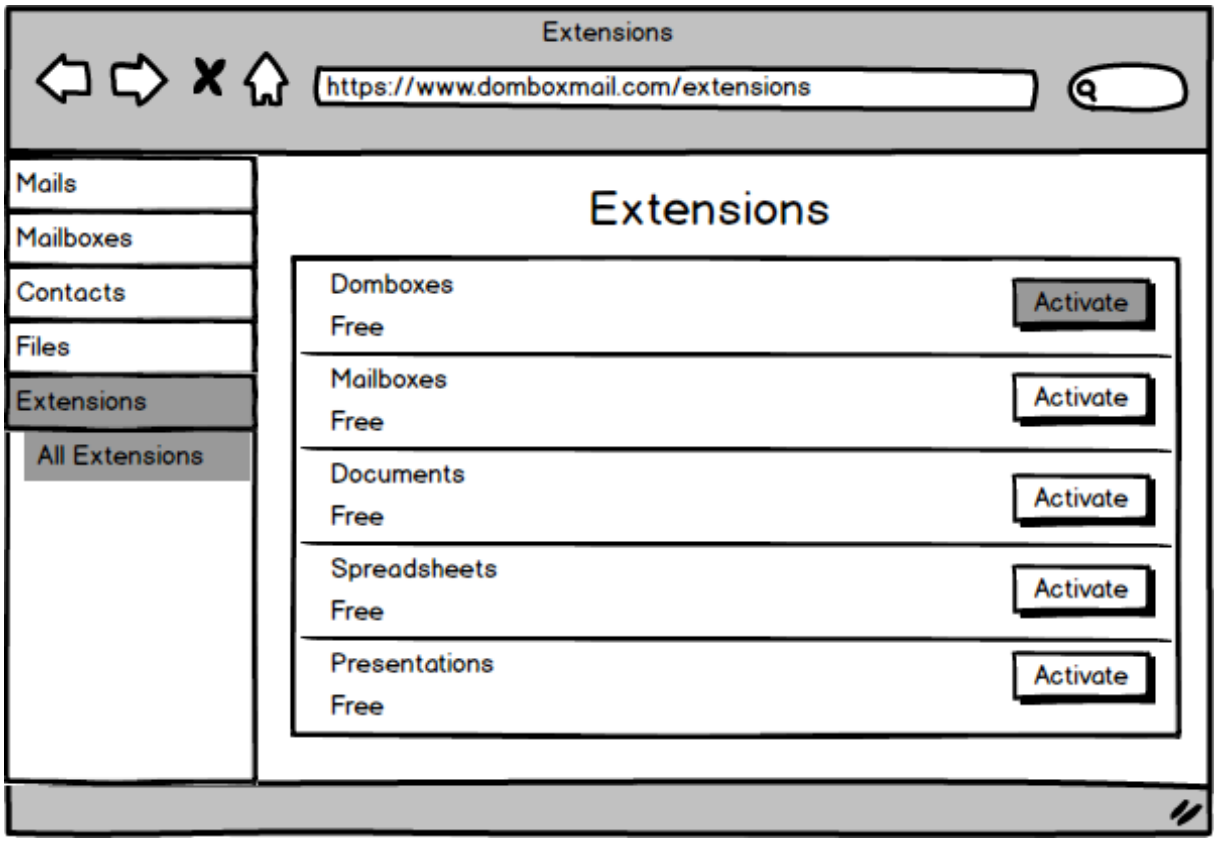


Figure 44: Domboxes Extension Activation

You must set the “Domkey”, before accessing the “Add Dombox” page.

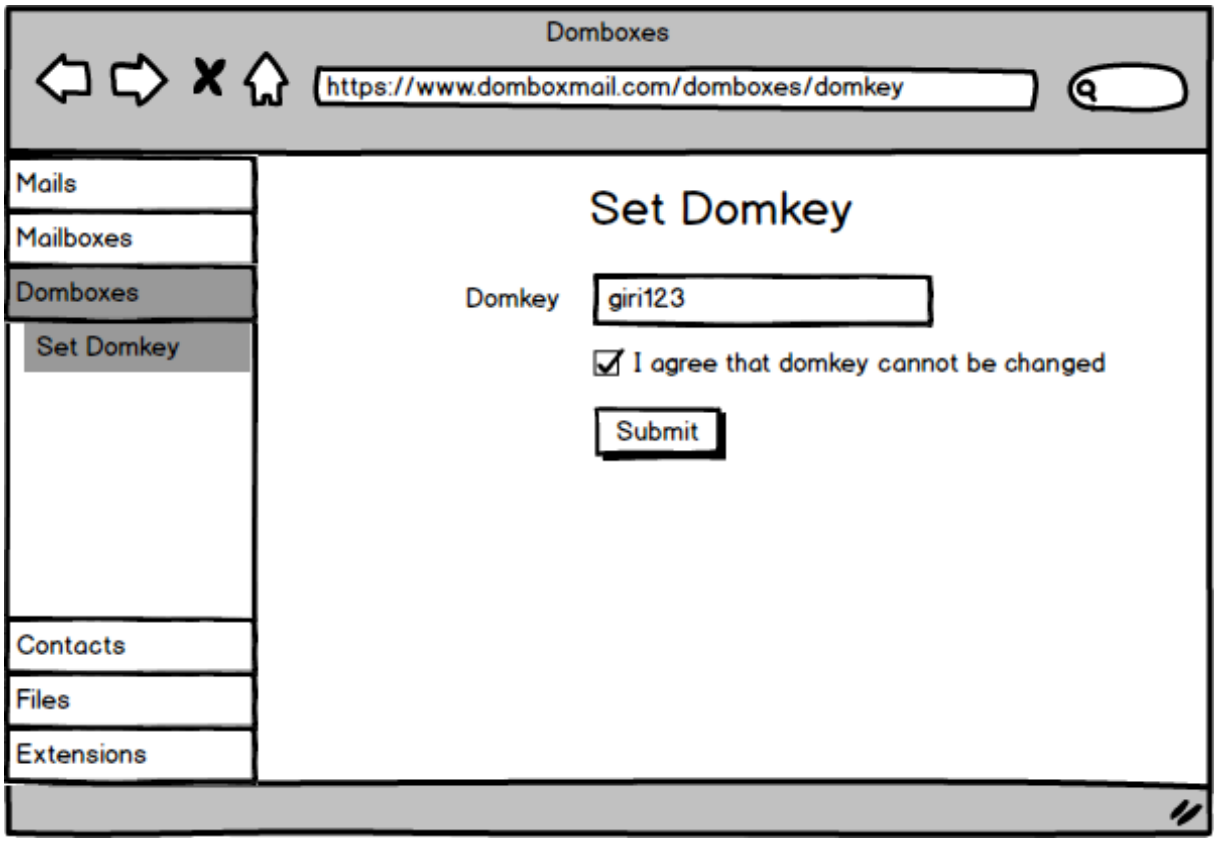


Figure 45: Set Domkey

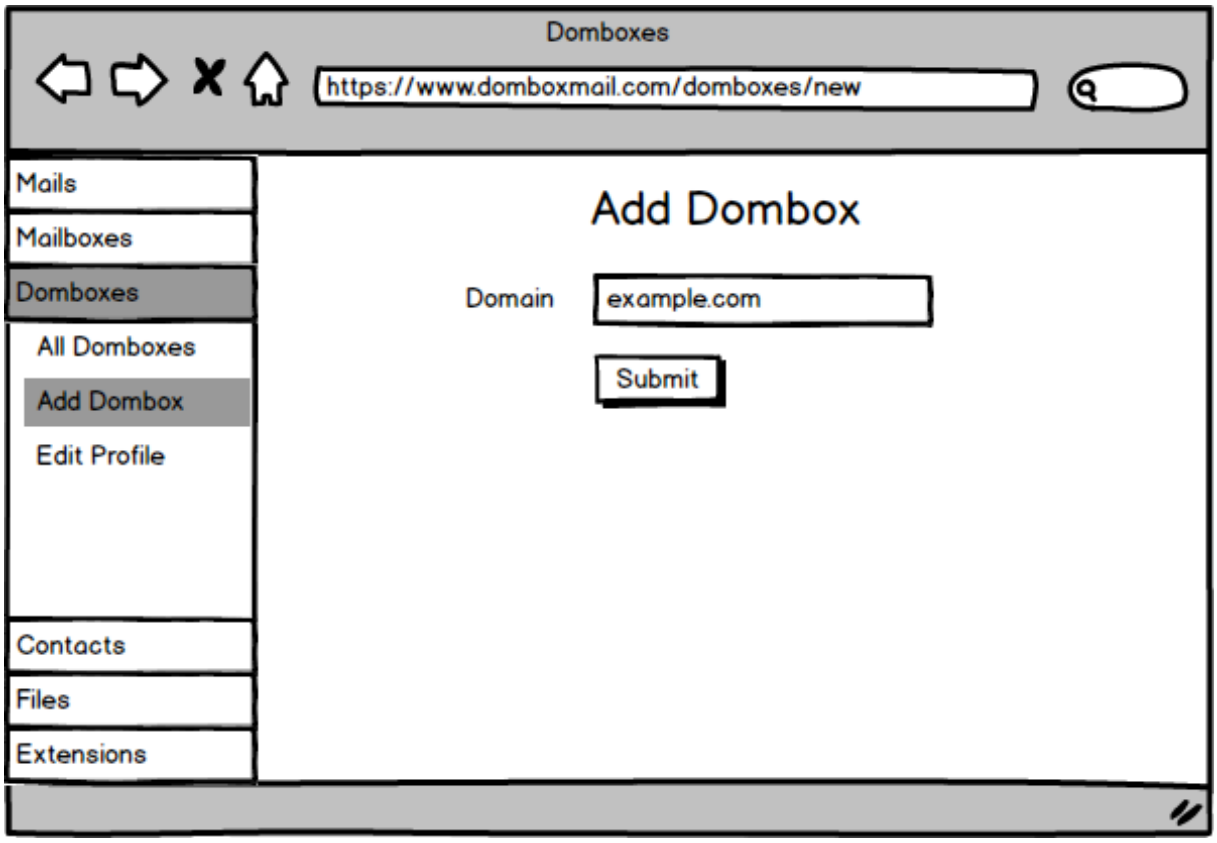


Figure 46: Add Dombox

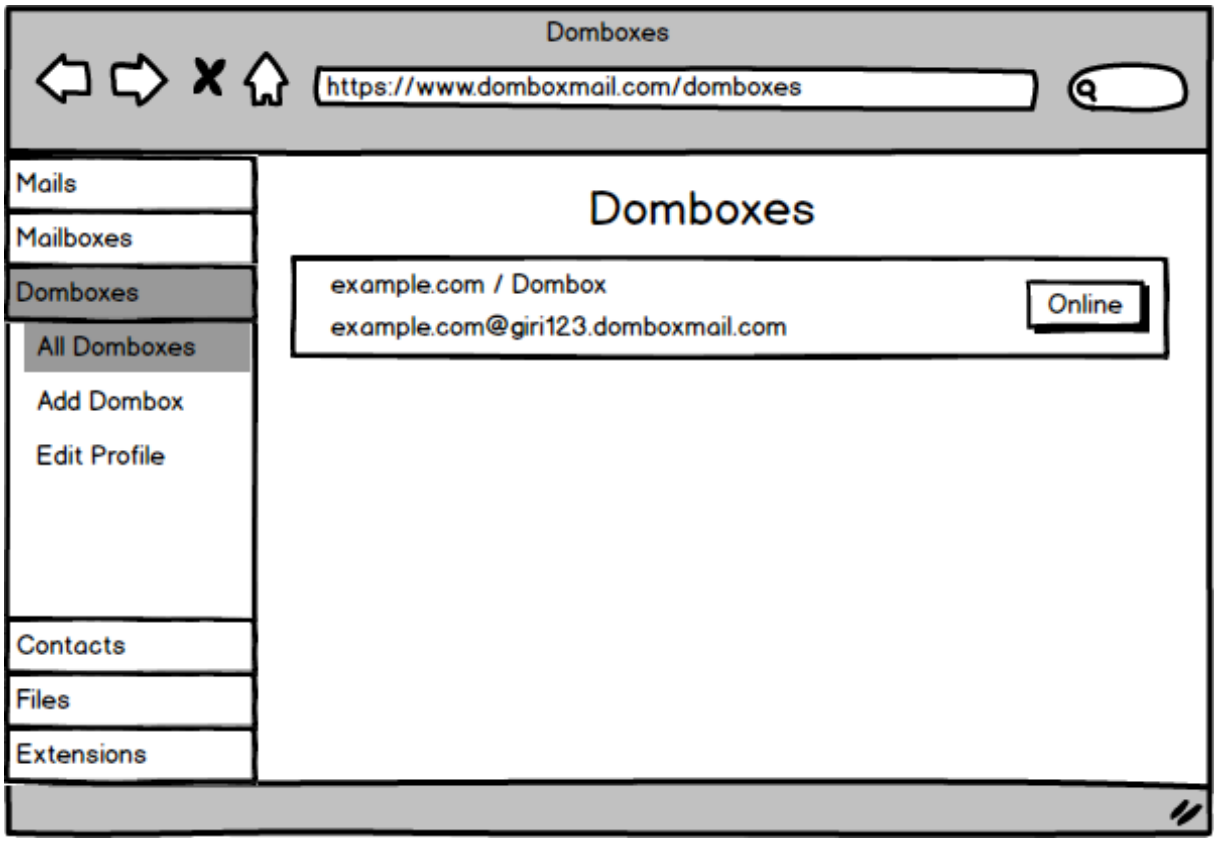


Figure 47: All Domboxes

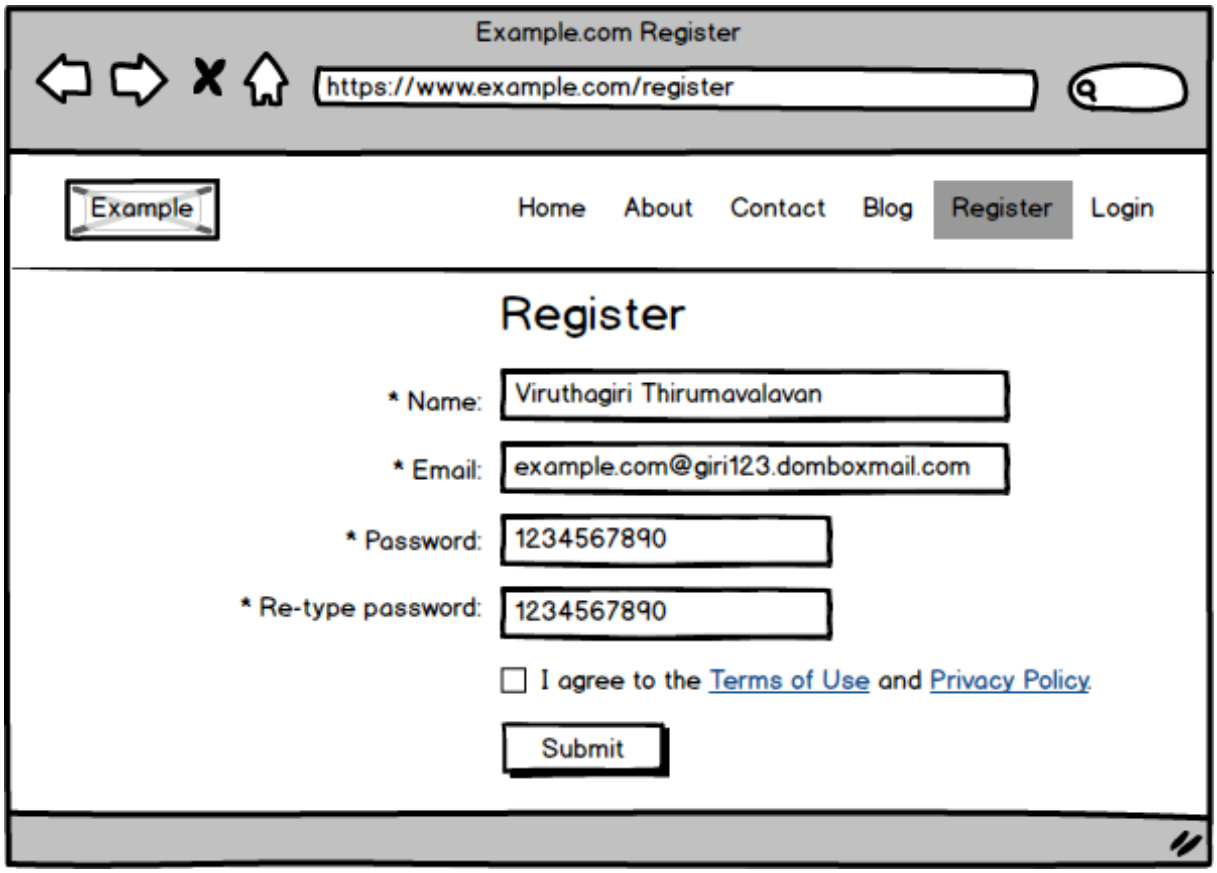


Figure 48: Use of Dombox Address on a Third Party Website

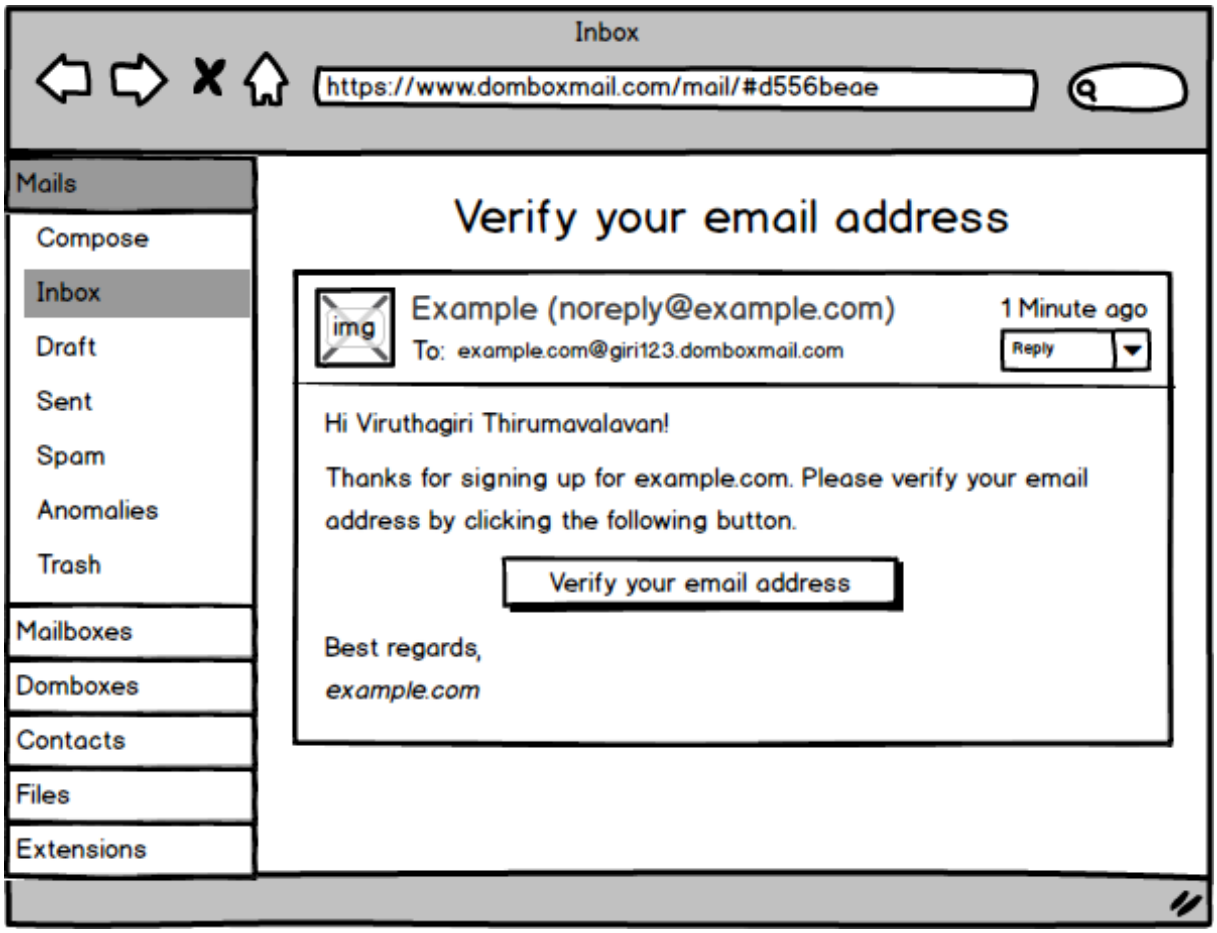


Figure 49: Mail received on a Dombox Address

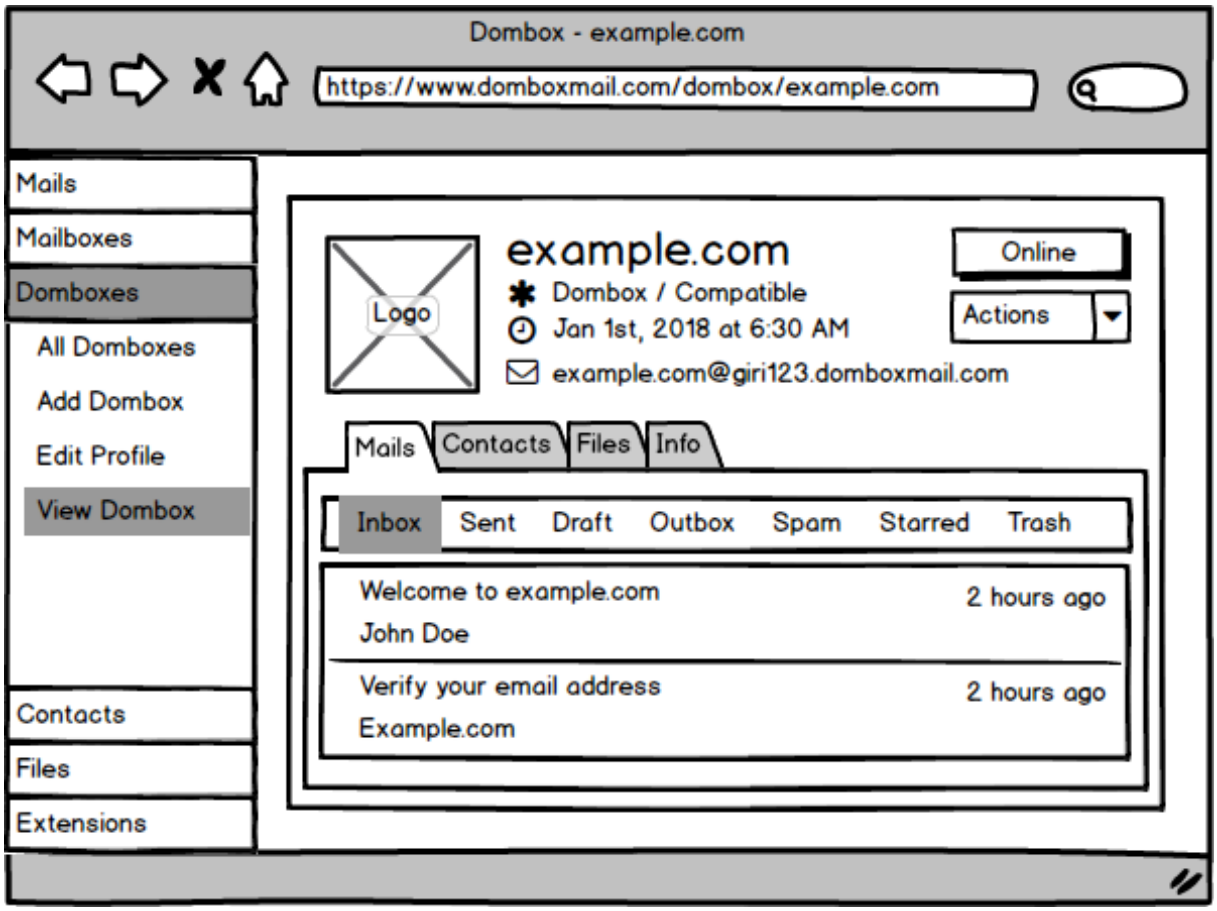


Figure 50: View Dombox - Mails Tab

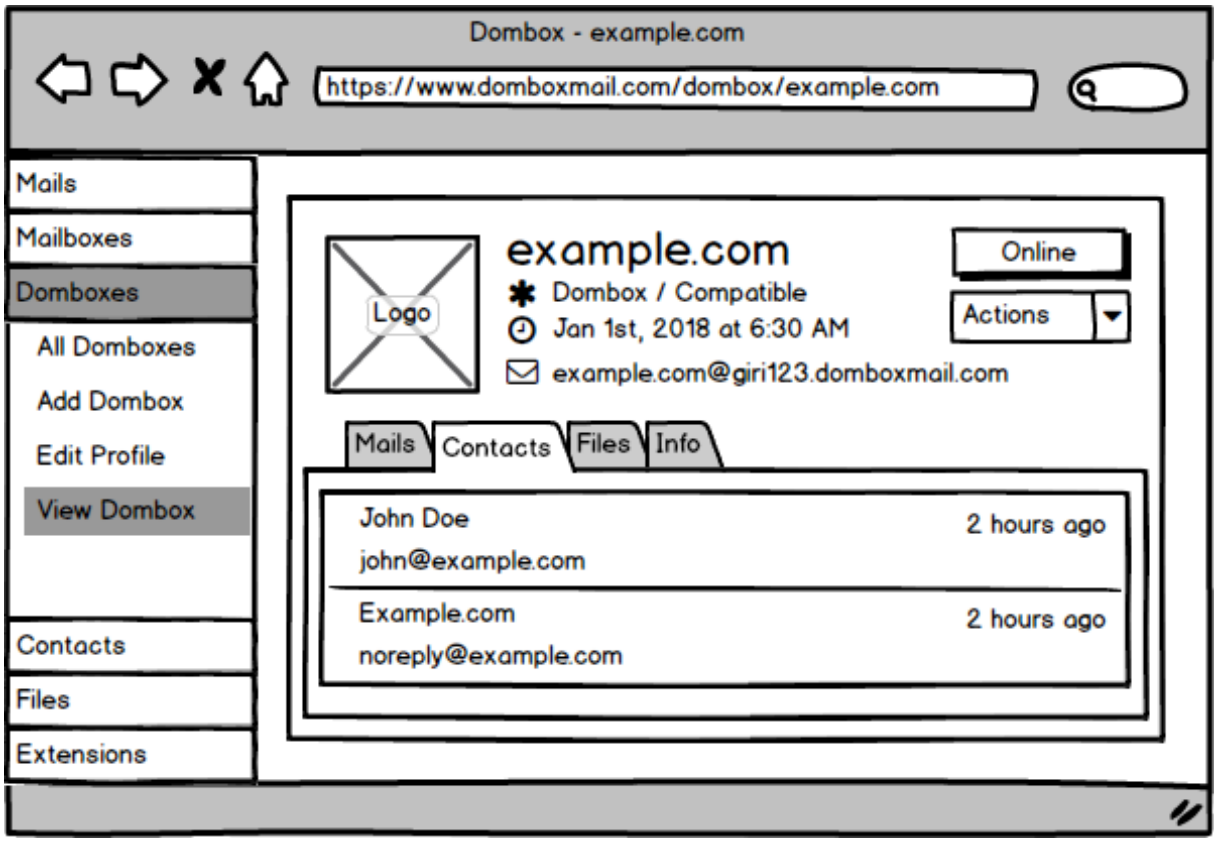


Figure 51: View Dombox - Contacts Tab

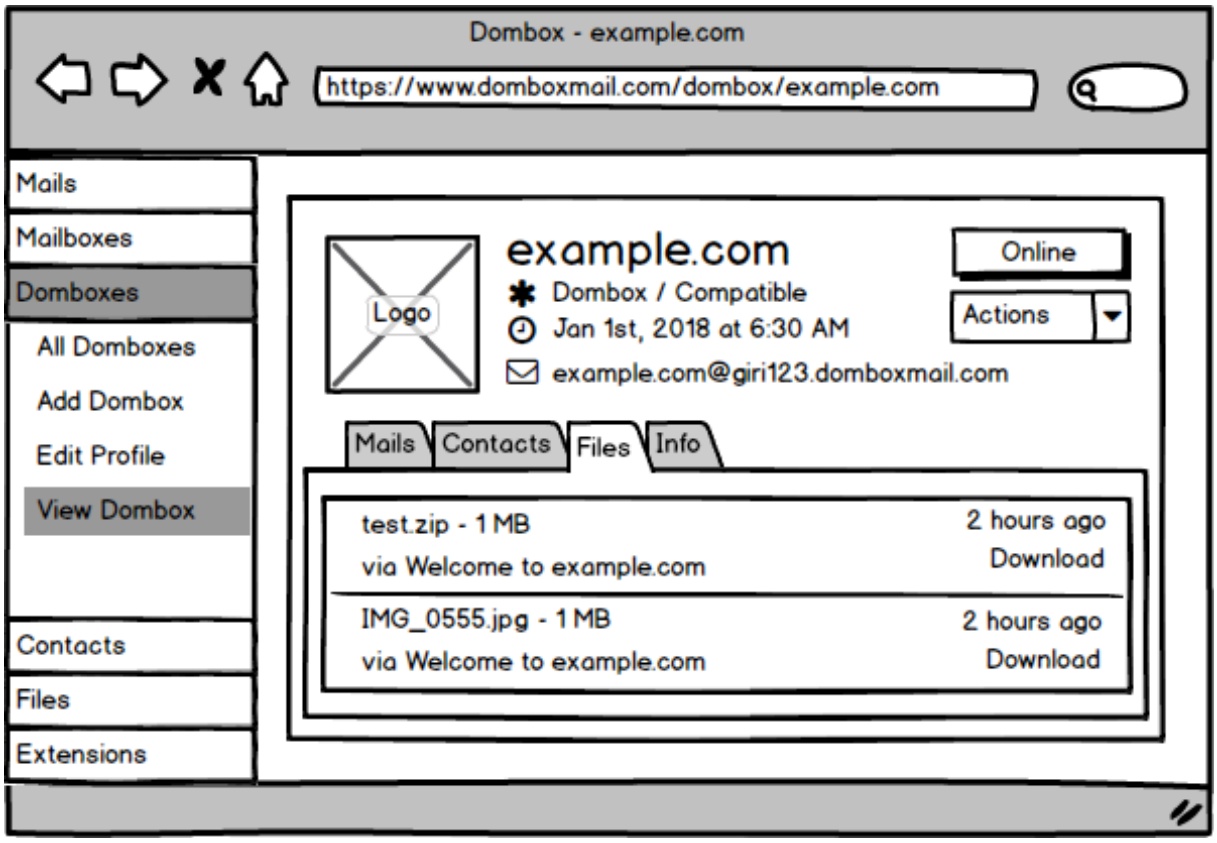


Figure 52: View Dombox - Files Tab

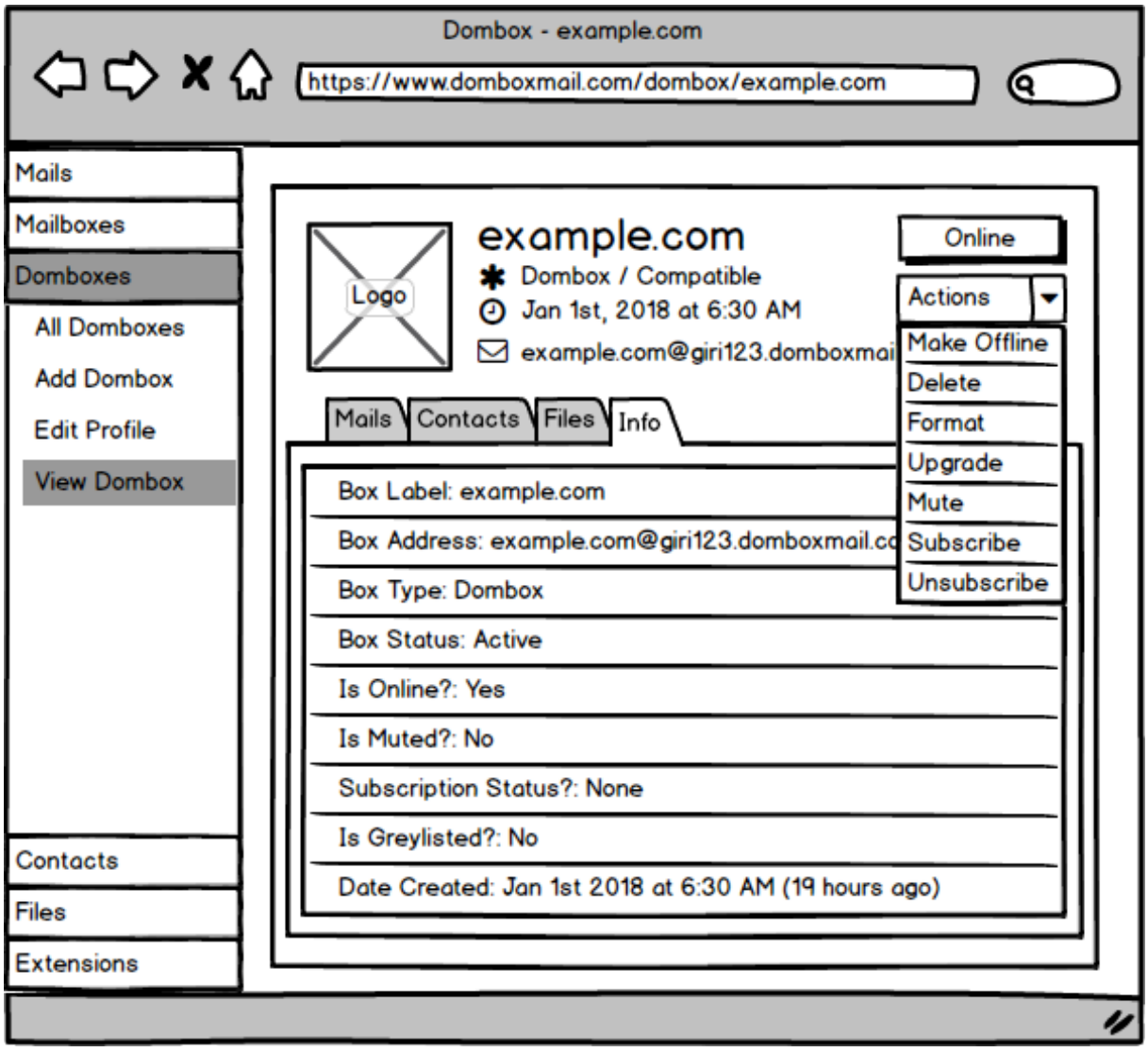


Figure 53: View Dombox - Info Tab

Chapter 10: Teleport

Unstable Users

By creating Dombox (D) we may have fixed the spam, but we created another problem. The consumers have full control of the box. The consumers can make their box offline or delete it completely anytime they want.

This may please the consumers but not the businesses. From the business perspective, these users are nothing but “Unstable Users”. i.e. They can disappear any time.

Recently Facebook’s privacy fiasco cost them billions of dollars. People started to delete their Facebook accounts. People who deleted their Facebook accounts also encouraged others to delete it using the #DeleteFacebook campaign.

Back In 2017, people were pissed about the way Uber doing business and started #DeleteUber campaign. Unlike Facebook, Uber is a Private Company. So the campaign didn’t do much damage. Uber only lost around 500,000 users.

Both campaigns would have had massive success if most of their users were Dombox users. Because we are letting the users to delete their box with a Single click.

Just for the record, Dombox is here to solve the spam problem. Not to jeopardize other businesses.

Dotcom Investors depends on metrics like “Number of Users” for valuing a company. So If we don’t solve the “Unstable Users” problem, then every business in the world gonna hate our mail service. So let’s solve that.

Combox (C)

The Combox (C) box type revokes the box deletion and box offline privileges from the consumer.

The term “Combox” refers to a Dombox that is under contract. In other words, Combox refers to a “Contract-based Dombox”.

The term “Contract” refers to an agreement between “Consumer” and the “Business”.

To initiate a Contract, business owners must register an App on our website and then they have to display a button on their websites

To register an App, business need to verify their domain first, since all contracts are linked to a particular domain

When a contract is signed, it also creates the Combox (C) for that contract automatically.

Combox (C) cannot be created from our website. A user needs to visit the third party website and then click our “Auth” button to initiate the “Contract”

The whole point of Combox (C) is that, the box can accept only the emails that pass all 5 layers. i.e. Score 5 mails

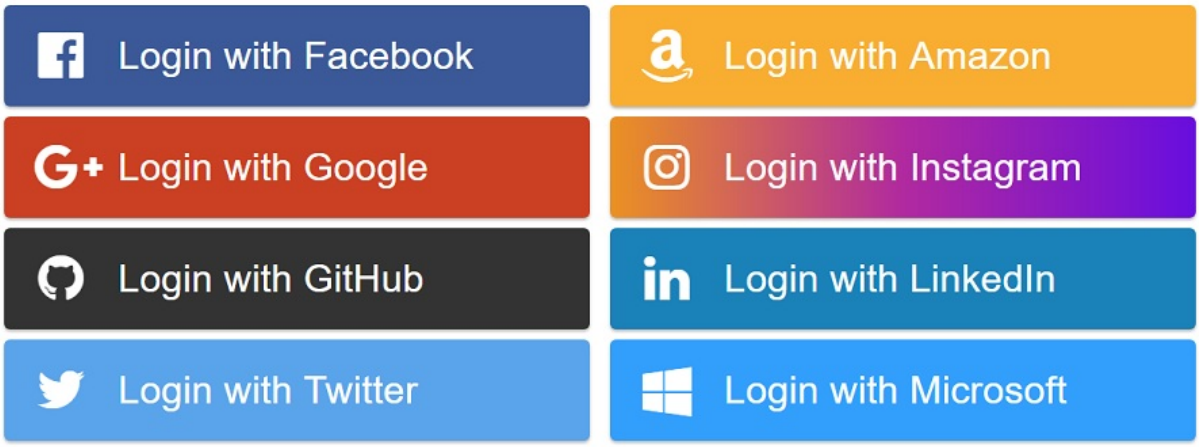
The business agrees to that part and we revoke the box deletion and box offline privileges from the consumer

Business Side: Stable Users

Consumer Side: Spam free Combox (C)

Auth Buttons

You probably have seen “Auth Buttons” like these on the Internet.



Hundreds of auth buttons like these available on the internet.

We are trying to bring an alternative to those buttons. Our “Auth Button” is called “Teleport”.

Other “Auth Buttons” are relying on e-mail address. But our “Auth Button” rely on i-mail address. So our “Auth Button” solves one major issue => Internet Privacy {Refer Chapter 19 for more info}

Let’s understand how our “Auth Button” works.

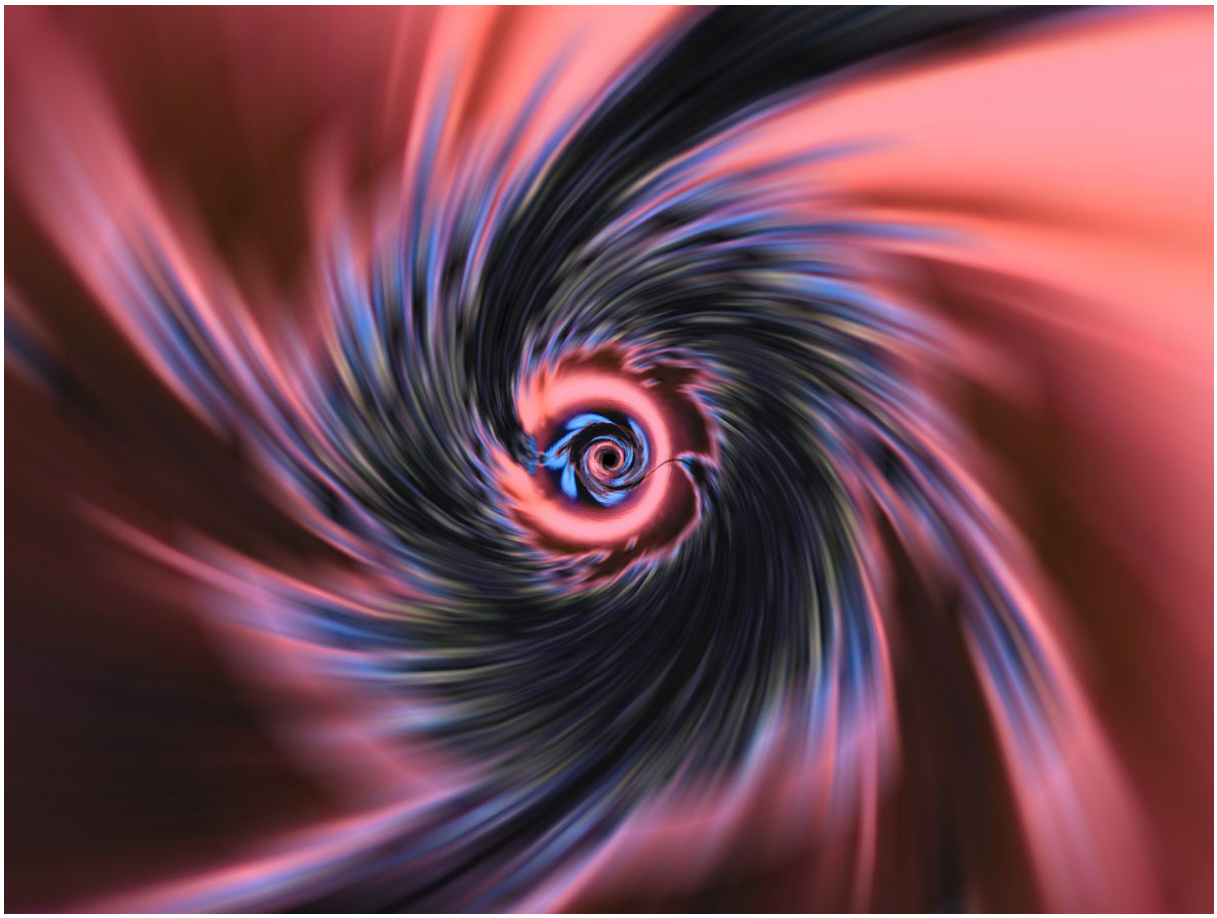
Portal

Portal can mean many things. e.g. Web portal. But we are using the term Portal in the science fiction context.

You might have seen the portals in movies. In the movie Avengers, they use a Vertical Portal to travel between planets. But in the movie Dr. Strange, they use Horizontal Portals to travel between places on earth.

We’re using the term “Portal” because the consumers save their time by skipping the process like filling registration forms, Creating a contract, Creating a Combox, Verifying emails etc. Consumers also skip the Login forms while logging in.

Teleport



The whole point of a portal is to travel quickly between two distant points.

You go through one door but come via another.

The process happening between these two doors is called “Teleportation”.

Definition from Wikipedia: Teleportation is the theoretical transfer of matter or energy from one point to another without traversing the physical space between them

Portal vs Teleport

We use both terms. “Portal” and “Teleport”. Keep in mind, The term “Portal” is intended for “Businesses” and The term “Teleport” is intended for “Consumers”.

Note for Developers: Please use the terminology exactly. e.g. Portal ID and Portal Secret. Don't call it Client ID, Consumer ID etc.

Business owners create the Portals. But it's the consumers who are gonna travel through them.

Take Facebook for an example, If you want to display "Signup with Facebook" button on your website, then you need to register your app first in Facebook and then you will have to display the "Signup with Facebook" button. So two things. App and Button

In Dombox Terminology, those "Apps" are called "Portals". And the button is called "Teleport"

If still, it doesn't make sense to you, the "Teleport" button is nothing but "Signup with Dombox" button

Parallel Internet

Every product needs a vision. Dombox is our core product and its vision statement is "A Spamless Internet". Dombox targets the consumers.

On the other hand, Teleport is our Authentication service and it targets the businesses. It's vision statement is "A Parallel Internet".

Don't take it in the wrong way. We are not trying to build a new Internet.

These days the term "Internet" lost its meaning to the "World Wide Web". So when we use the term "A Parallel Internet", some people may expect a new kind of browser, a new HTTP alternative protocol etc.

But the truth is, calling "World Wide Web" as "Internet" is nothing more than calling the "Angry Birds" app found in your phone as "iPhone". iPhone is the platform and the app leverages that platform to provide its services.

"Internet" stands for "Interconnected Computer Networks" and when we use the term "A Parallel Internet", we are talking about a "Interconnected Computer Networks" that revolves around our "i-mail addresses" as opposed to traditional "e-mail addresses".

We are gonna have two very important teams in our company. (1) Team “Dombox” (2) Team “Teleport”

Team “Dombox”:

Team	Dombox
Audience	Consumers
Location	domboxmail.com
Vision	A Spamless Internet
Focuses On	Mails, Mailboxes, File Management, Spam Filters, Virus Scanners, Advanced Search, Productivity, Developing tools to automate the Isolated Mailbox creation and update process in third party websites.
Can help with questions like	What is Dombox? How mail score works? What is Restricted Mode? {The term “Restricted Mode” will be explained in a later section}

Team “Teleport”:

Team	Teleport
Audience	Businesses
Location	domboxmail.net
Vision	A Parallel Internet
Focuses On	Teleport, Telescribe, Portal App Registration (OAuth2 based), Portal Clients (develops and distributes portal client libraries for all popular languages, CMS and frameworks)

Team	Teleport
Can help with questions like	What is Combox? What is Teleport? What is Telescribe? How to achieve the level 5 mail score? How to configure Teleport?

So the Team “Teleport” is driven by the vision “A Parallel Internet” and their primary job is developing and distributing the “Teleport” and “Telescribe” button to every website on the internet.

The following figure represents the Present Internet

Figure 54: The Present

This is how we want the future to look like (A decade from now and yes it's an ambitious one)

Figure 55: The Future

Others button - Popup view

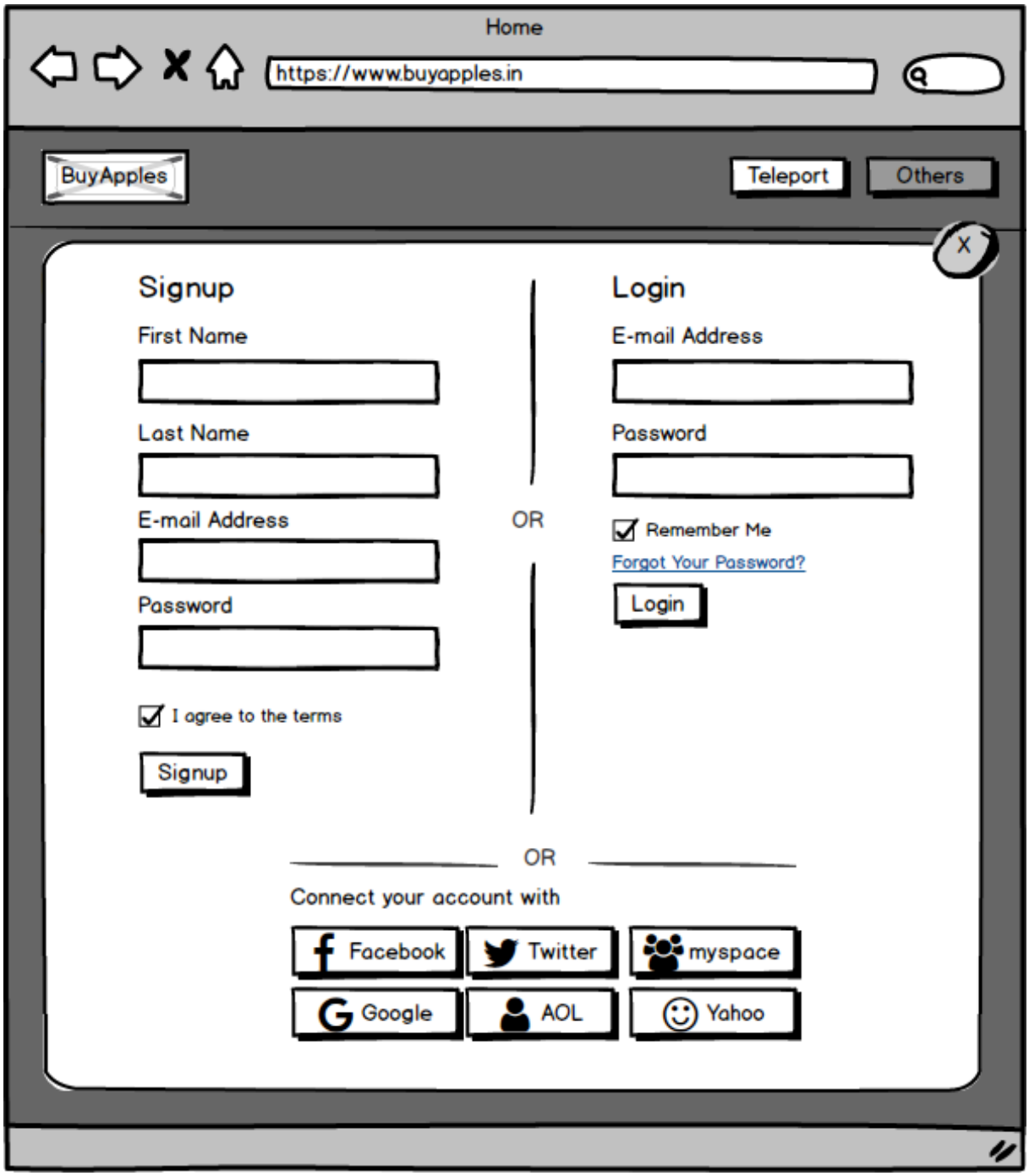


Figure 56: Popup view

Official Domains

Domain	Audience
domboxmail.com	Consumers
domboxmail.net	Businesses
dombox.org	Employees
investor.dombox.org	Investors

So far, we were talking from the “Consumer” perspective. So we used the domain “domboxmail.com”.

From this point forward, we are gonna talk from the “Business” perspective. So we are gonna use “domboxmail.net”

Add Domain

Domain Verification

If you are a business owner you need to verify your domain first before creating a portal.

Step 1: Click “Add New Domain”

Step 2: Enter the domain

Step 3: Copy the randomly generated Verification string and Paste it in your DNS record.

Step 4: Come back and then click on the “Process Verification” button.

If the exact random verification string found in your domain DNS, then you are the rightful owner. So the domain will be marked as “Verified”

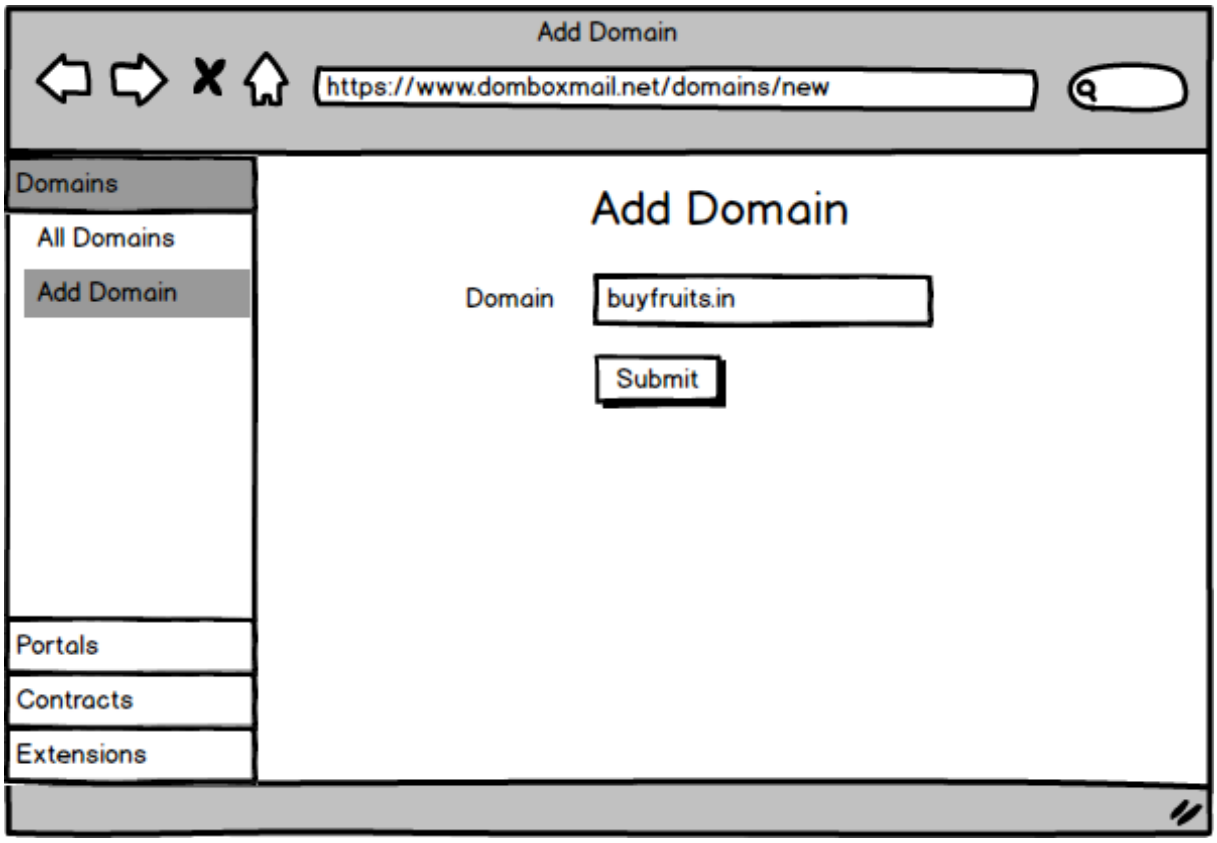


Figure 57: Add Domain

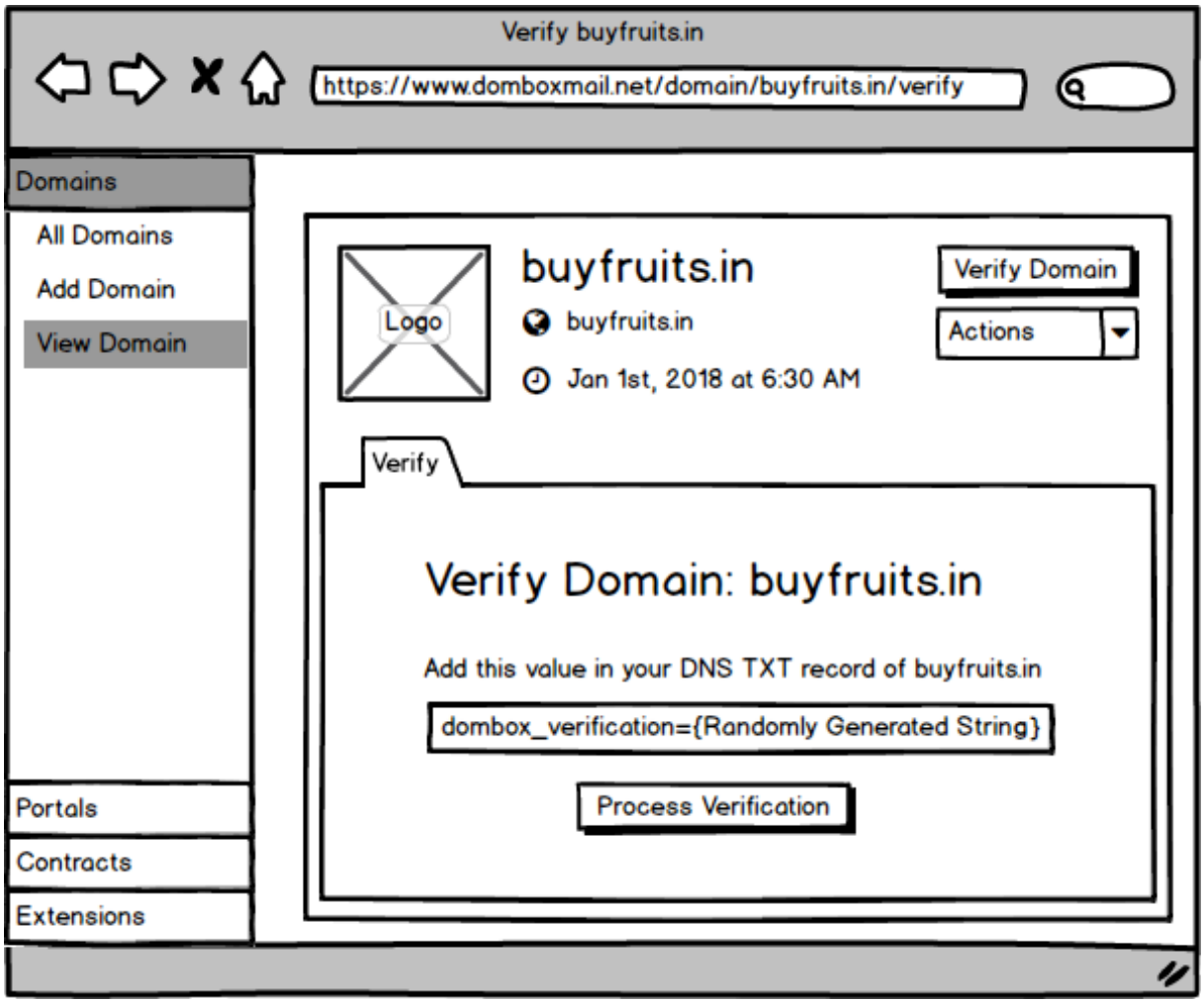


Figure 58: Verify Domain

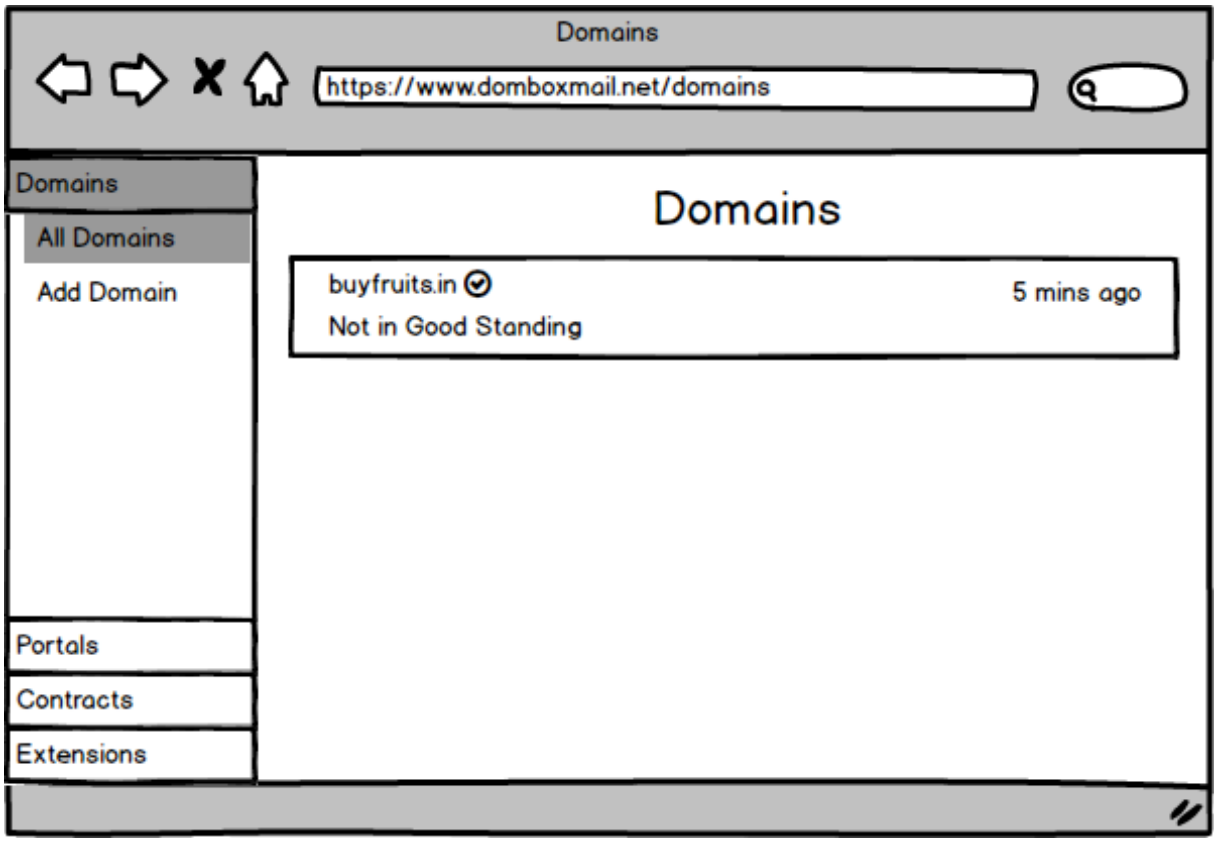


Figure 59: All Domains

Good Standing

If you are a business owner, the deal is very simple. You send only verified emails to the "Combox" and in exchange, we remove the box deletion and box offline privileges from the box.

Underline the words "verified mails". That's your bargaining chip. So you need to prove us that your domain really passes all the 5 layers by sending an email to the randomly generated email address.

After verification, the system will give you the "Good Standing" status. But keep in mind, you still need to comply with some of the terms to keep the "Good Standing" status. For

example, if your domain keeps sending malicious mails even after passing 5 layers, then you may lose the “Good Standing” status.

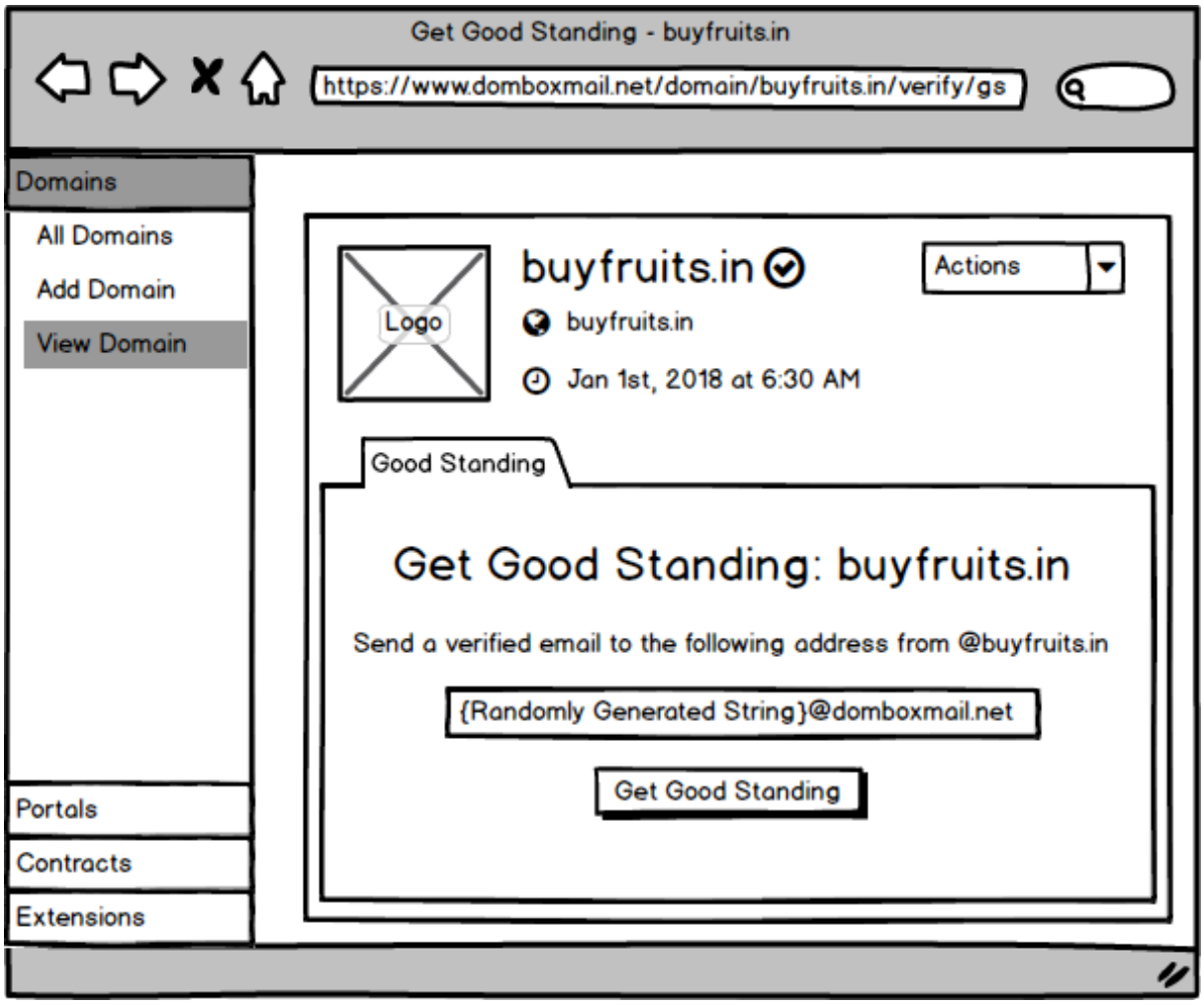


Figure 60: Get Good Standing

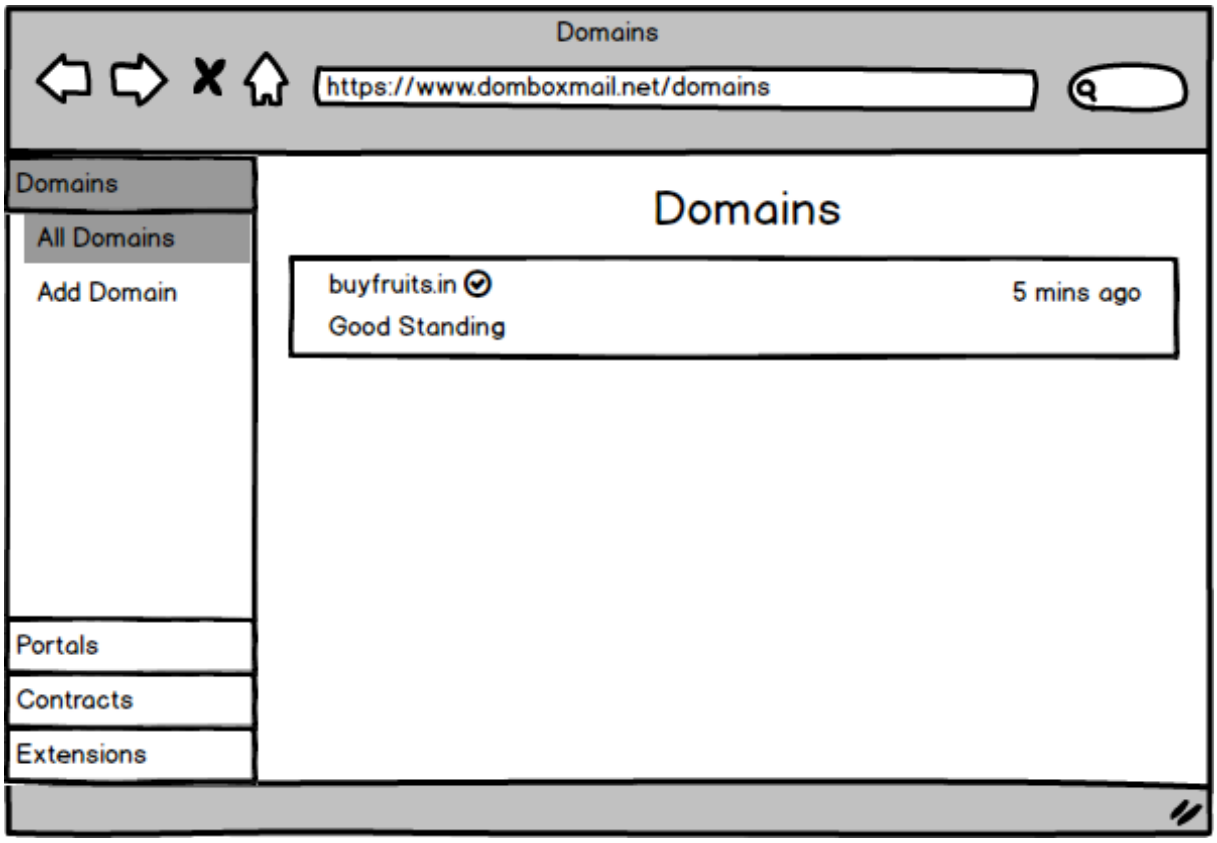


Figure 61: Good Standing Domain

Add Portal

Select Domain

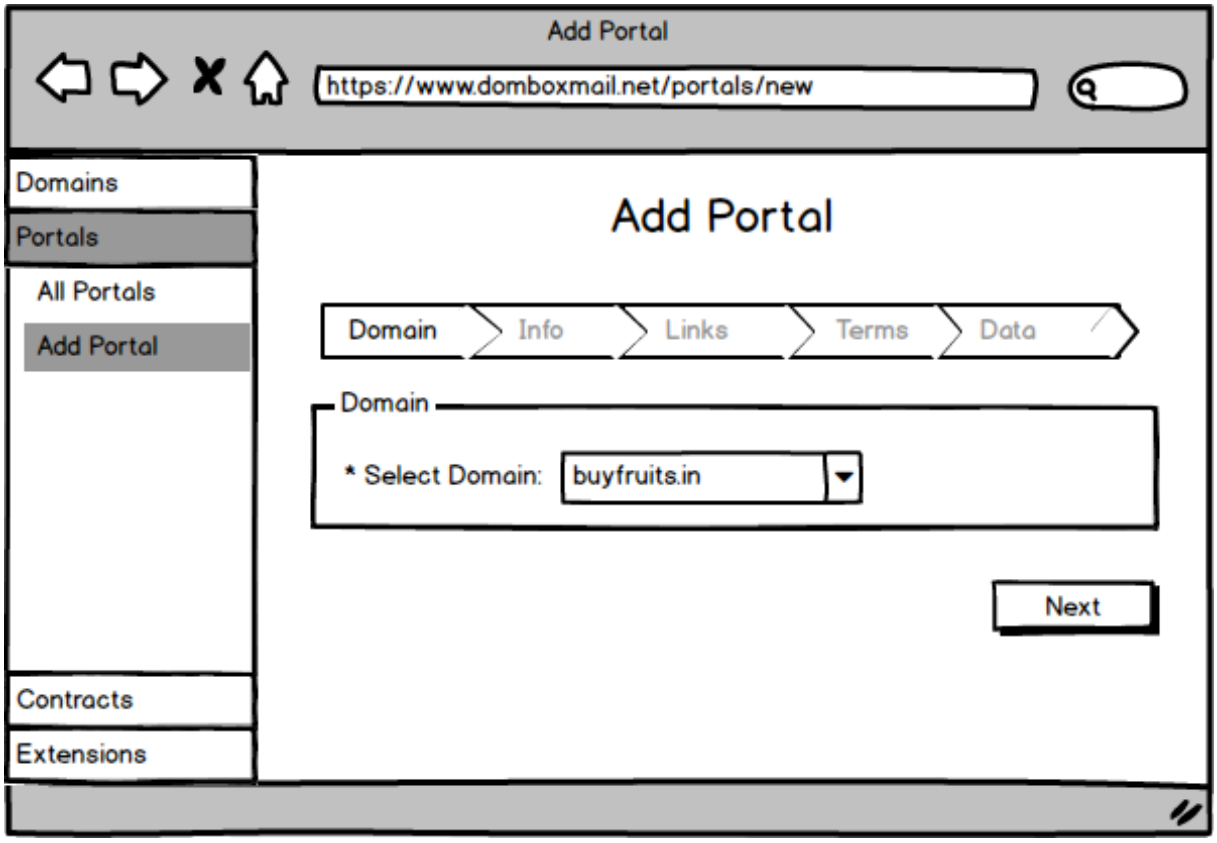


Figure 62: Select Domain

Portals cannot be created for unverified domains.

Portals cannot be created if the domain doesn't have the "Good Standing" status

Every portal will be linked to a domain.

In the select domain page, the business owner needs to select the domain from the domain field. Only verified domains with good standing, are available for selection.

In the last image, buyfruits.in is selected for the domain

Portal - Info

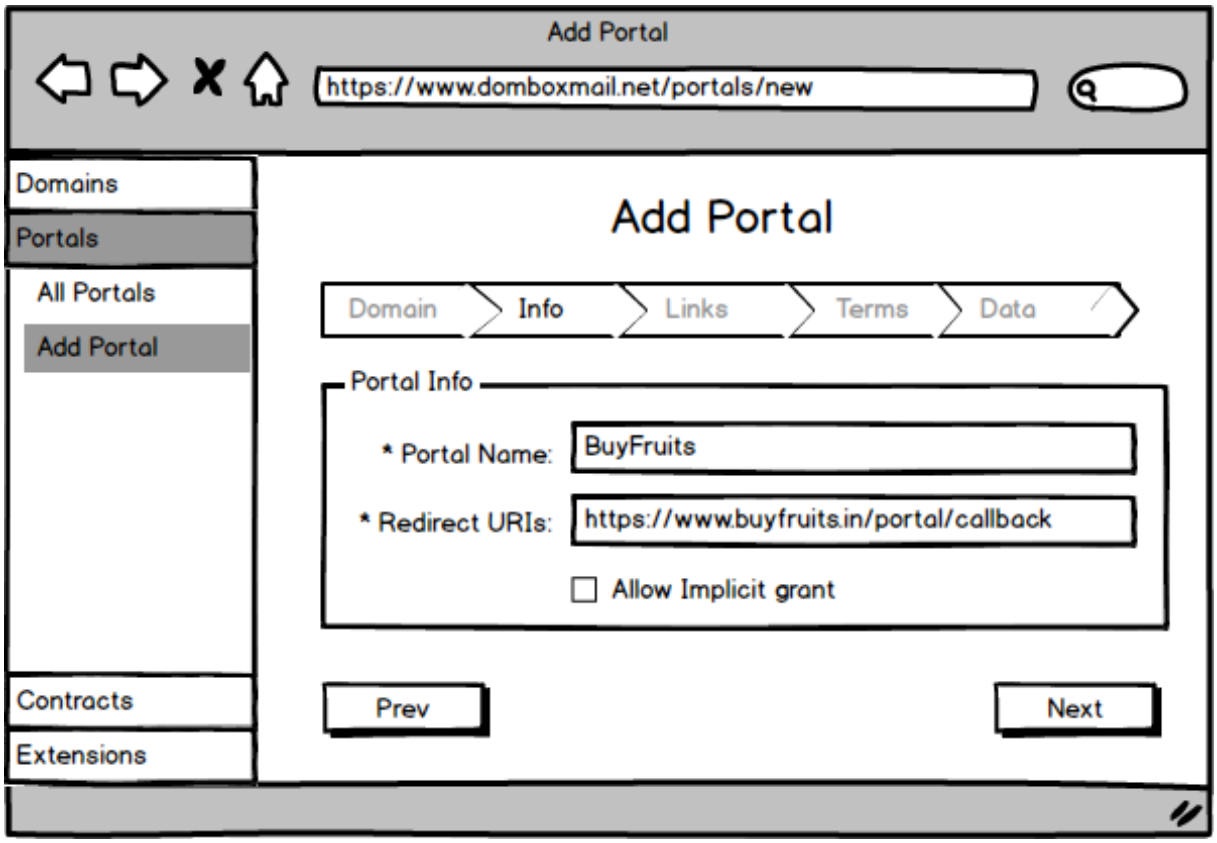


Figure 63: Portal Info

In Portal Info page, the business owner enters the Portal Name and Redirect URIs.

A domain can have unlimited portals. But for most domains, only one portal is enough. For example, an educational website can have a portal for students and another portal for teachers. To prevent confusion, the business owner should give a portal name to identify the portal properly.

For security reasons, all portals must have at least one Redirect URIs. The business owner needs to provide that.

If you have any plans to deploy the portal app in Native mobile applications or Javascript only applications, then it requires “implicit grant” in order to work. In such cases, the Business Owner can Opt-In by checking the “Allow Implicit Grant” checkbox.

Note: Check “Allow Implicit Grant” checkbox, only when you need this option. Implicit Grant provides low security. This is disabled by default for security reasons.

Portal - Site Links

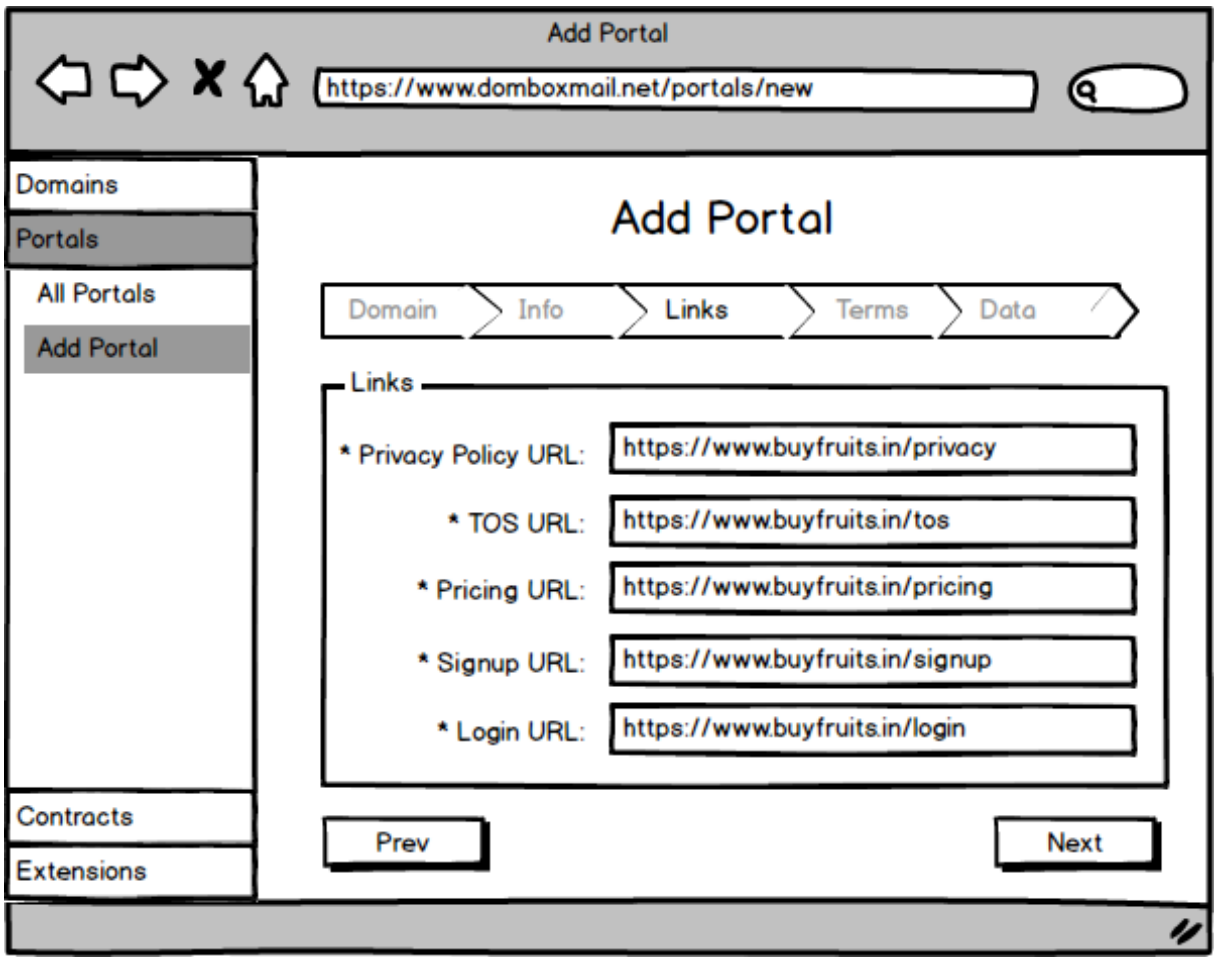


Figure 64: Portal - Site Links

In the Site Links page, the business owner enters the relevant site links.

These links will be displayed to consumers. So they can check the links before signing up to the website.

The Business owner should provide the Privacy Policy Page URL, Terms Of Service Page URL, Pricing Page URL, Signup Page URL and Login Page URL.

The Signup Page URL and Login Page URL are the urls where the “Teleport” button can be found.

Note: Once the domain become our “Portal Partner”, we disable the “Add Dombox” functionality for the domain and then ask our users to signup/login via the “Teleport” button found in those URLs

Portal - Contract Terms

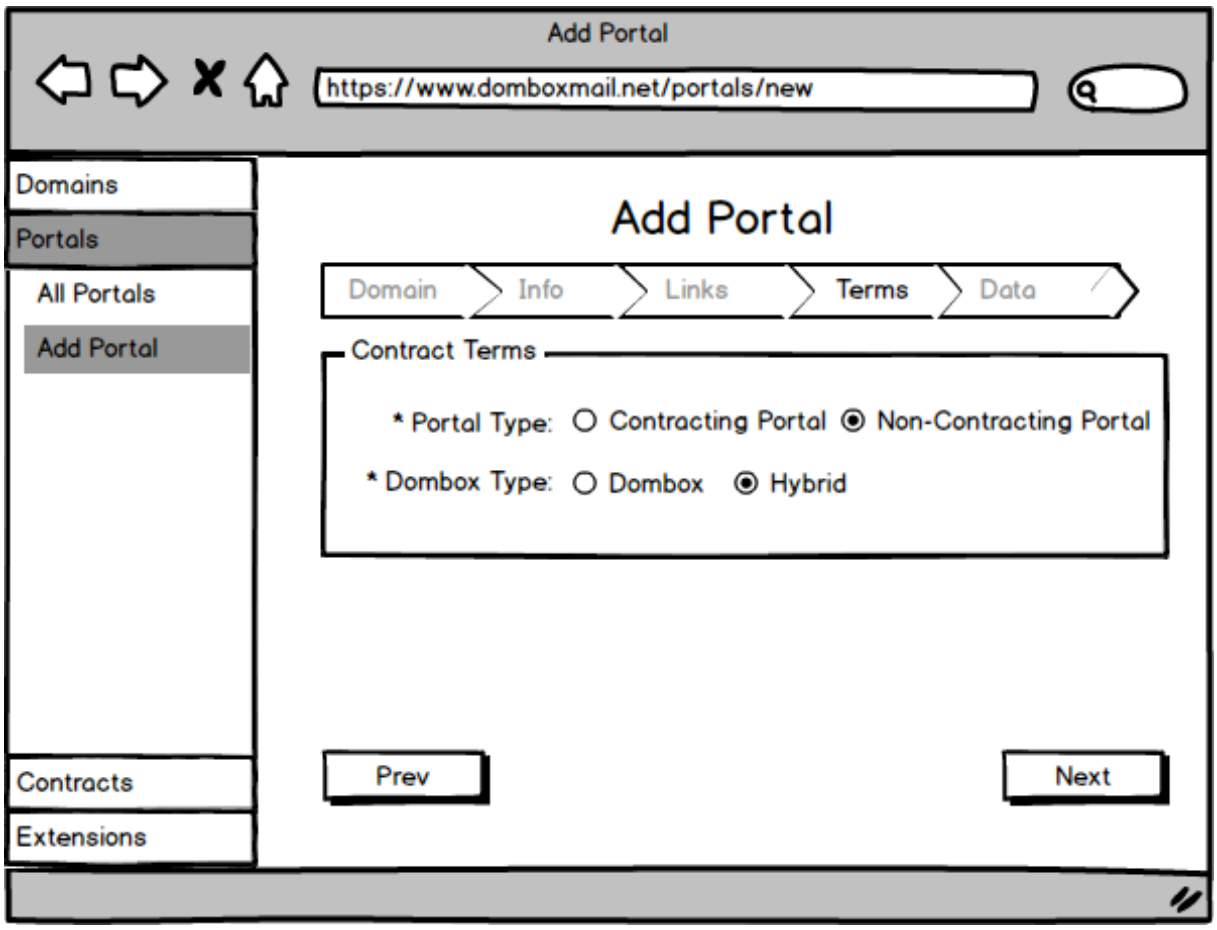


Figure 65: Non-Contracting Portal

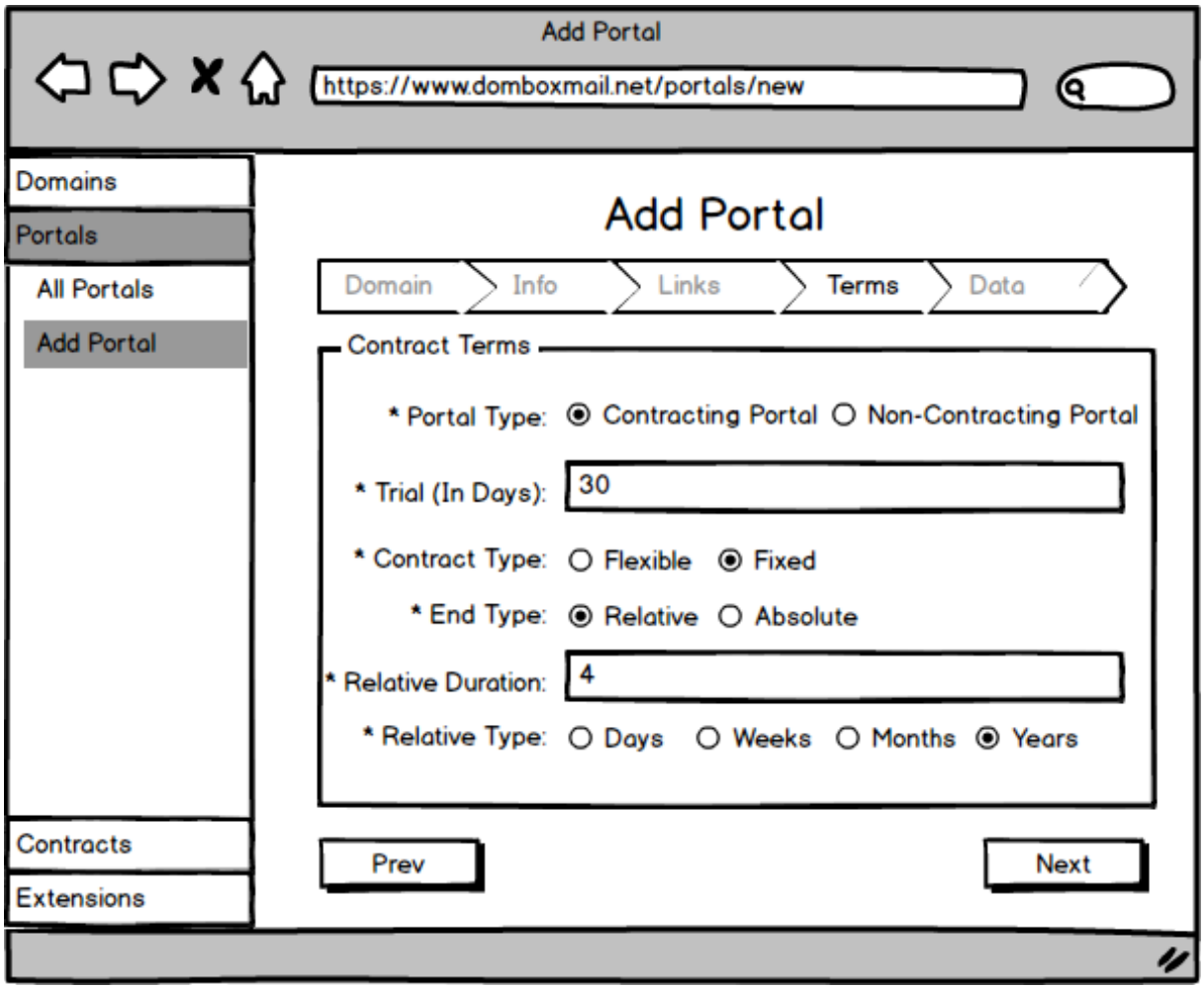


Figure 66: Contracting Portal

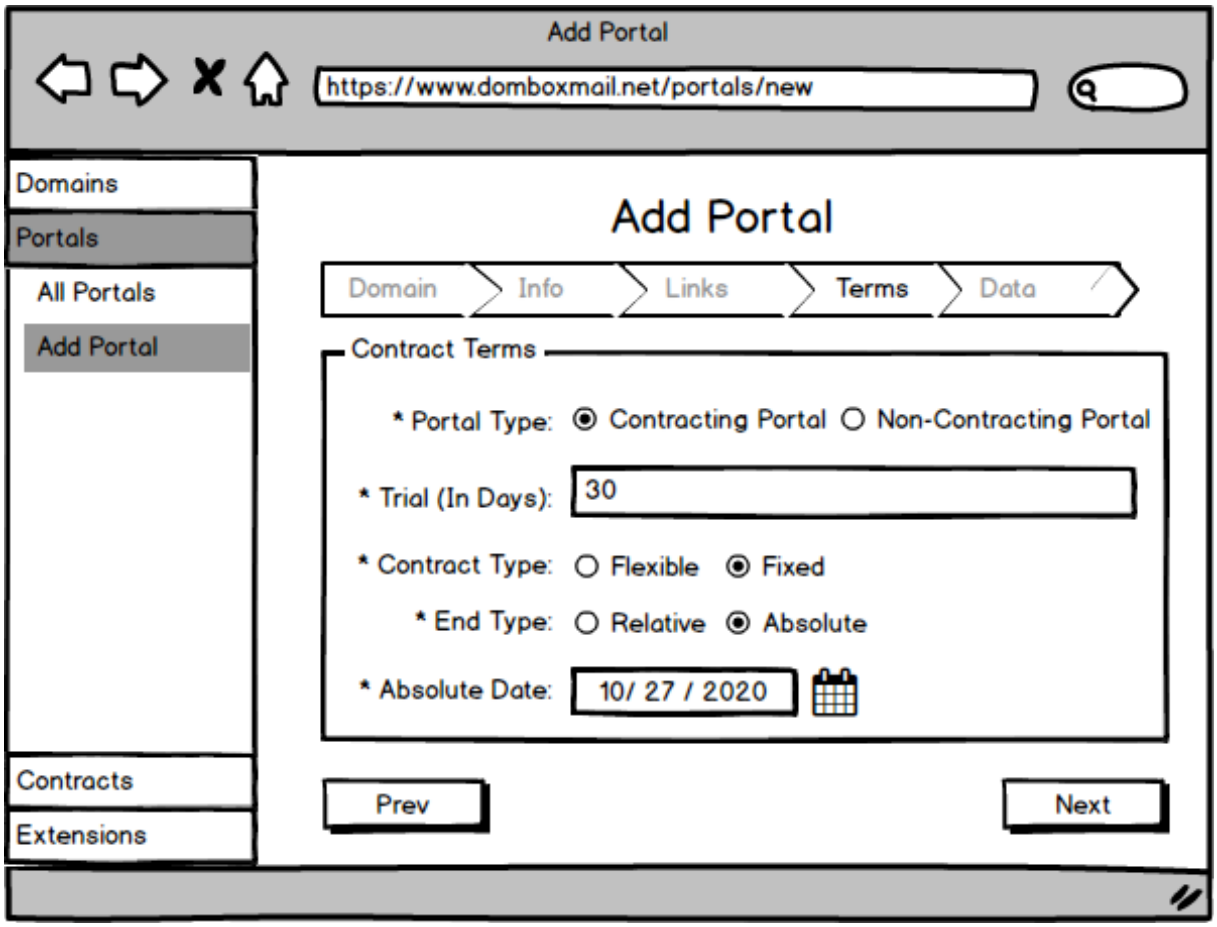


Figure 67: Absolute End Type

Portal - Required Data

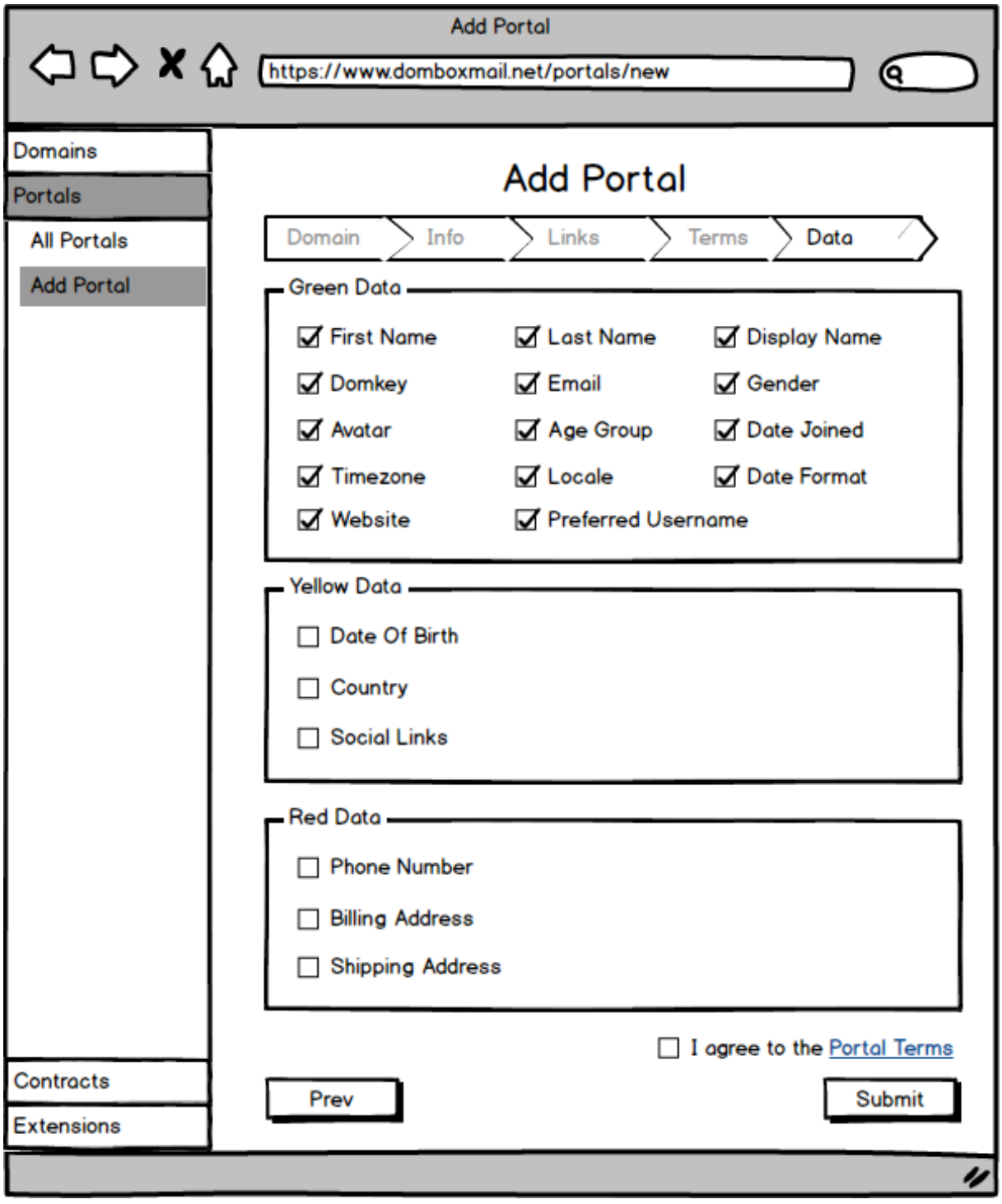


Figure 68: Green Data

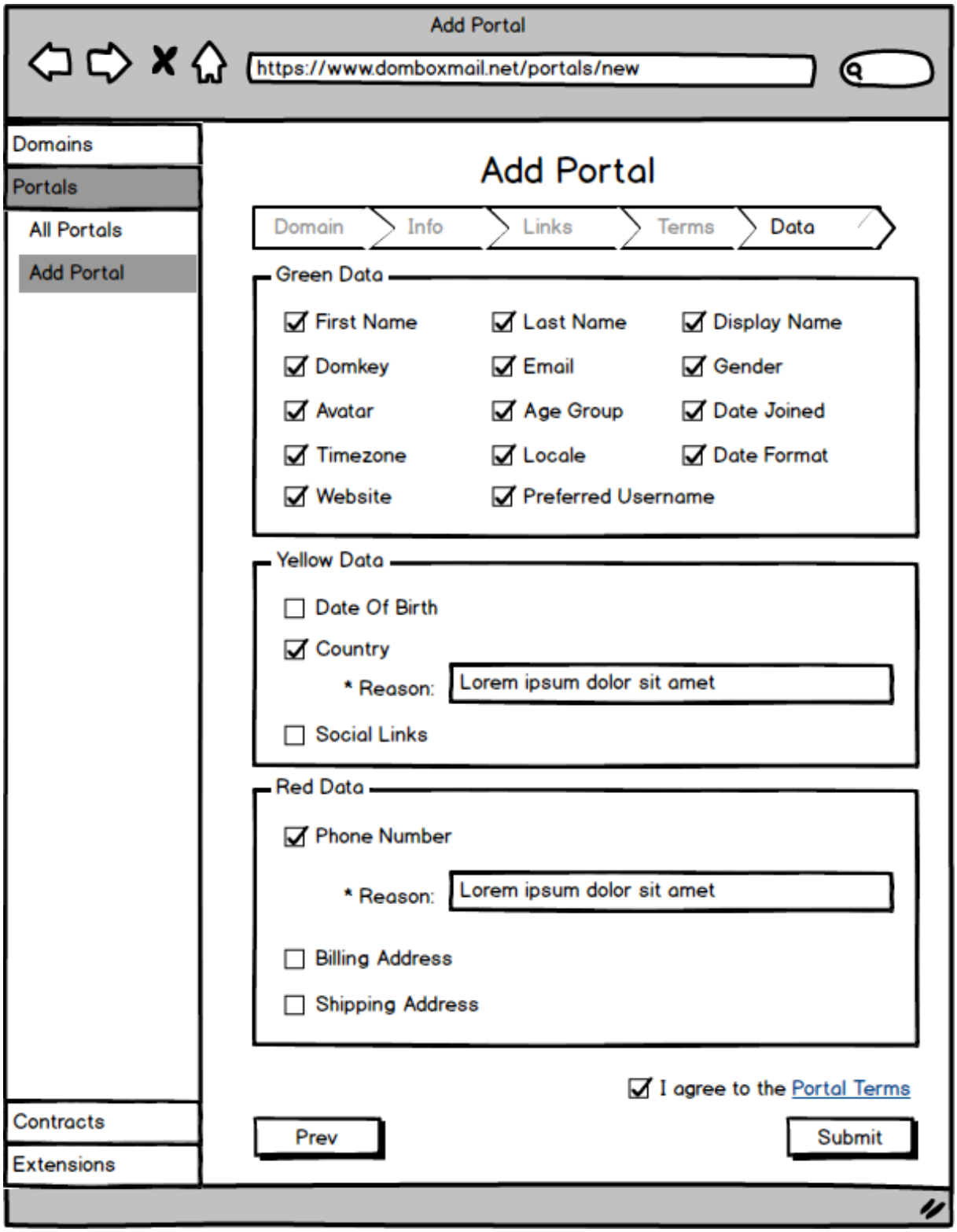


Figure 69: Yellow & Red Data

Portal Types

Type	Description
Contracting Portal	Intended for Combox (C) box type
Non-Contracting Portal	Intended for Dombox (D) and Hybrid (H) box types

Contract Types

Type	Description
Flexible Contracts	Flexible contracts have “no end date”. We’ll explain later why its called Flexible contract.
Fixed Contracts	Fixed contracts have an “end date”. The end date can be either relative or absolute.

Fixed Contracts - Relative

Relative end type contracts have the “same duration” for all contracts regardless of the signup date.

The best use case for relative end type contract is a student web portal.

Priya, Khan, and David they are all trying to signup for a 2 years course.

Priya’s course starts on Jan 2018 and ends on Jan 2020. Khan’s course starts on Jan 2019 and ends on Jan 2021. Davids’s course starts at Jan 2020 and ends on Jan 2022

As you can see they all have the same duration regardless of the signup date. In this case, they are all on contract for 2 years.

In relative end type, you need to provide a relative duration. The relative duration can be in Days, Weeks, Months and Years.

e.g. 30 days from the signup date, 5 weeks from the signup date, 6 months from the signup date, 2 years from the signup date.

Fixed Contracts - Absolute

Absolute end type contracts has “variable duration” for all contracts.

The best use case for absolute end type contract is a music concert.

Let’s just say Katy Perry has a music concert in Dec 2020 and the event organizer would like to keep in touch with the online ticket buyers till the concert date. In this case, the event organizer can go for absolute end type contract.

Priya buys the concert ticket on Jan 2018. Khan buys the concert ticket on Jan 2019. David buys the concert ticket on Jan 2020

But all their contracts end on Dec 2020 once the concert is over.

If you do the math, Priya is on contract for 3 years, Khan is on contract for 2 years and David is on contract for 1 year. So the duration is not the same in absolute end type contracts.

In absolute end type, you need to provide the exact date. e.g. “31 Dec 2020”

Trial

By default, the Trial days is set to zero days. i.e. No Trial. However, a website can set a Trial to a higher value (Ex: 30 days) to attract more customers to try their product.

Think about it. When a website advertises like “30 days Money back guarantee”, they may return your money, but they are still keeping your email address. That means the website can contact you any time in the future. They can also sell your email address to spammers.

But If the website also advertises like “30 days Teleport trial”, that means the website is giving you some sort of “No strings attached guarantee”. You can “Cancel” the contract within the trial period.

When you cancel the contract, the box instantly goes to “Offline”.

For the sake of our example, let’s assume there is a Note Taking website called AwesomeNotes.com

The website owner of AwesomeNotes believes people are gonna love his product if they try his product for just 10 minutes. So the website owner sets the Trial Days to “30 Days” to attract more users.

Priya sees this “No strings attached guarantee” and she understands that she can walk away anytime without receiving any annoying emails from the website owner. Since she got nothing to lose, she uses our “Teleport” button and voila, within a matter of seconds she is now a proud member of AwesomeNotes.

Priya Signed Up on “01, Jan 2020” and the Trial ends on “30, Jan 2020”

Priya clicks the “Cancel Contract” button on Jan 10. The box goes “Offline”. She can’t put the box “Online” unless she continues the contract. Note: If the box is “Offline”, all incoming emails will be rejected. So “Offline” boxes are “Read-Only” boxes.

10 Days later Priya decided to continue the contract. So she clicks the “Continue Contract” button on Jan 20. The “Cancel Contract” button still available till Jan 30. She can cancel the contract anytime before Jan 30. But if 30 days passed since her signup date, then the “Cancel Contract” button won’t be available.

However, when the box is in “Cancelled” status, the “Continue Contract” will always be available even after the trial days. If Priya clicks the “Continue Contract” button on Feb 20 instead of Jan 20, then she can’t cancel the contract anymore.

Note: Whether it’s a “Flexible Contract” or “Fixed Contract”, all contracts can have the Trial.

Maximum Possible Contract Length

Answer these questions…

What’s preventing a website owner from setting the relative duration value to “2000 years” instead of “2 years”?

What's preventing the music concert organizer from setting the absolute date to the year "Dec 3020" instead of "Dec 2020"?

We cannot ask our users to stay on contract for 1000 years. Can we? That would be crazy right?

So whether it's a Fixed contract or Flexible Contract, all Contracts must have a maximum duration. This is what we call "Maximum Possible Contract Length"

The formula for "Maximum Possible Contract Length" calculation is

> $L_{max} = H_{max} - A_{min}$

Where L_{max} = Maximum Possible Contract Length (in Days)

Where H_{max} = Longest known human lifespan in History (in Days).

Where A_{min} = Minimum age required to signup for Dombox mail service (in Days).

H_{max} is the longest known human lifespan in History (in Days). This value is constant. Jeanne Louise Calment[67] from France holds the current Guinness record[68] for the title "Oldest Person Ever". She was born on 21 February 1875. Died on 04 August 1997. So her lifespan 44,724 days is used as the value.

This constant value 44724 cannot be changed until someone else break that Guinness record. The new record holder must be officially replaced the old record holder in Guinness world records to modify this constant.

A_{min} is the minimum age required to signup for our mail service. The value should be in Days. This value is a constant too. At this moment a person should be 13 years old to signup for our mail service. Although the minimum age requirement may vary based on the user's country, we are gonna stick with the US standard for this one.

To calculate the Days, we use the first 13 years of Jeanne Louise Calment. So it would be treated like she joined our mail service when she turned 13 and used it till her death. The number of days from 21 February 1875 to 21 February 1888 is used to calculate this value.

[67] https://simple.wikipedia.org/wiki/Jeanne_Calment
[68] http://www.guinnessworldrecords.com/world-records/oldest-person-(female)

So the value is 4,748 days. i.e The first 13 years of her age. This value cannot be changed until our mail service minimum age requirement for the US get changed.

L_{max} = 44724 - 4748

L_{max} = 39976

Maximum Possible Contract Length in Days: 39976 Days

Maximum Possible Contract Length in Years: ~ 109.5 Years

Both “Absolute” contracts and “Relative” contracts must comply with “Maximum Possible Contract Length”.

The relative end duration can be in Days, Weeks, Months and Years.

If the relative end duration is in days, the maximum value is 39976 Days.

If the relative end duration is in weeks, the maximum value is 5710 weeks.

If the relative end duration is in months, the maximum value is 1314 months.

If the relative end duration is in years, the maximum value is 109 years.

The “Absolute end date” must be an exact date. When the website owner set this date while creating a Portal, the end date cannot be a date that is greater than 39976 days from the current date.

Initial Duration

There are websites out there that goes out of business within a year of their launch date.

Now, What would happen to those people who had signed up in such websites if they were actually under a contract? The website is gone, but the users are still locked in their contracts. Right?

If we tell the users that they have to wait 109 years to delete the box, they are gonna be furious. On the other hand, If we let them delete their box, and if the website owner put his website back online, say 15 years later, then our company will be in trouble. Because users are gone but 109 years contract length has not over yet.

To solve this problem, whether its a “Flexible Contract” or “Fixed Contract”, all contracts comes only with an Initial Duration and the website need to earn the remaining duration by renewing them (by sending a mail that passes all 5 layers).

Two types of Initial Duration available.

Initial Duration for “Good Standing” => 5 years

Initial Duration for “Combox” => 5 years

Renewal

All Contracts must be renewed by the domain and not by the user.

Two types of renewal required for all contracts.

1. Global Renewal
2. Local Renewal

Global Renewal

The business must send at least one “5 layers passed mail” from the “Dombox Domain” every five years to any mail account in our mail system to keep the “Good Standing” status. This is called “Global Renewal”.

All renewals come with a 5-year extension.

If a domain gets “Good Standing” status for the first time in Jan 1st, 2020, its valid till Jan 1st, 2025. To get a 5-year extension (i.e Till Jan 1st, 2030), at least one 5 layers passed mail must be sent between Jan 1st, 2020 to Jan 1st, 2025.

The point of “Global Renewal” is to make sure the website is an active one and not out of business.

Note: The value “5 years” may get changed in the future.

Local Renewal

When a contract is signed by the consumer, the “Combox” comes with a 5-year duration.

The business must send at least one “5 layers passed mail” every five years to the “Combox” to extend the contract by 5 more years. This is called “Local Renewal”.

e.g. If a contract is signed by the consumer on Jan 1st, 2020 it’s valid till Jan 1st, 2025. If the business sends at least one “5 layers passed mail” between Jan 1st, 2020 to Jan 1st, 2025 then the contract is renewed till Jan 1st, 2030.

The point of “Local Renewal” is that, to make sure the user doesn’t have any stalled (inactive) boxes for a long time.

Note: For Global Renewal “5 layers passed mail” must be from the “Dombox Domain” to be considered as valid. But for “Local Renewal” mail from “SAD Domains” are considered valid too.

Also note, “Local Renewal” depends on “Global Renewal”. i.e. If the business is not in “Good Standing” status, then the “Local Renewal” won’t happen

Duration vs Renewal

The “Duration” part and the “Renewal” part may cause some confusion

Let us clarify them here

The maximum possible contract length is 39976 Days

When we use the term “Flexible Contract”, we are actually referring to a contract that expires 39976 days from the signup date. i.e. The full possible duration

If you are website owner and you have no idea whether you should pick “Flexible Contract” or “Fixed Contract” for contract type, you should always pick the “Flexible Contract” type

You should pick “Fixed contract” type only on special cases like Student course, Music concert etc. In a nutshell pick “Fixed Contracts” only for short-term contracts.

Again… When in doubt, Always go with “Flexible Contract” type.

Although “Flexible Contracts” have full possible duration, it only comes with an initial duration. The website needs to keep on renewing them by sending emails. That’s why its called Flexible contact.

In a way, Fixed Contracts also same as Flexible contracts. What makes them “Fixed” is the “end date”.

For the sake of our example, Let’s say both the Initial Term and the Renewal Term is 10 years. That means the flexible contract needs at least 10 renewals in the 109 years

e.g. Contract Signed in the year 2000. The flexible contract is valid until the year 2109. But the initial term comes with only 10 years. If the website sends at least one mail in between 2000 to 2010, then its renewed till 2020. If the website sends at least one mail in between 2010 to 2020, then its renewed till 2030 and so on

Same rules apply to “Fixed Contracts” but the renewal happens until the “end date” set by the website owner.

Deadlock

Once you create your first Portal, you are officially our “Portal Partner”.

When a site becomes our “Portal Partner” that usually means they are displaying the “Teleport” button and that site requires a contract to create a Combox. In such cases, Consumers cannot add a Dombox via “Add Dombox” page.

If they enter a “Portal Partner” domain in the “Add Dombox” page, they will get a message like this.

“buyfruits.in is our Portal Partner. Please use the Teleport button to signup”

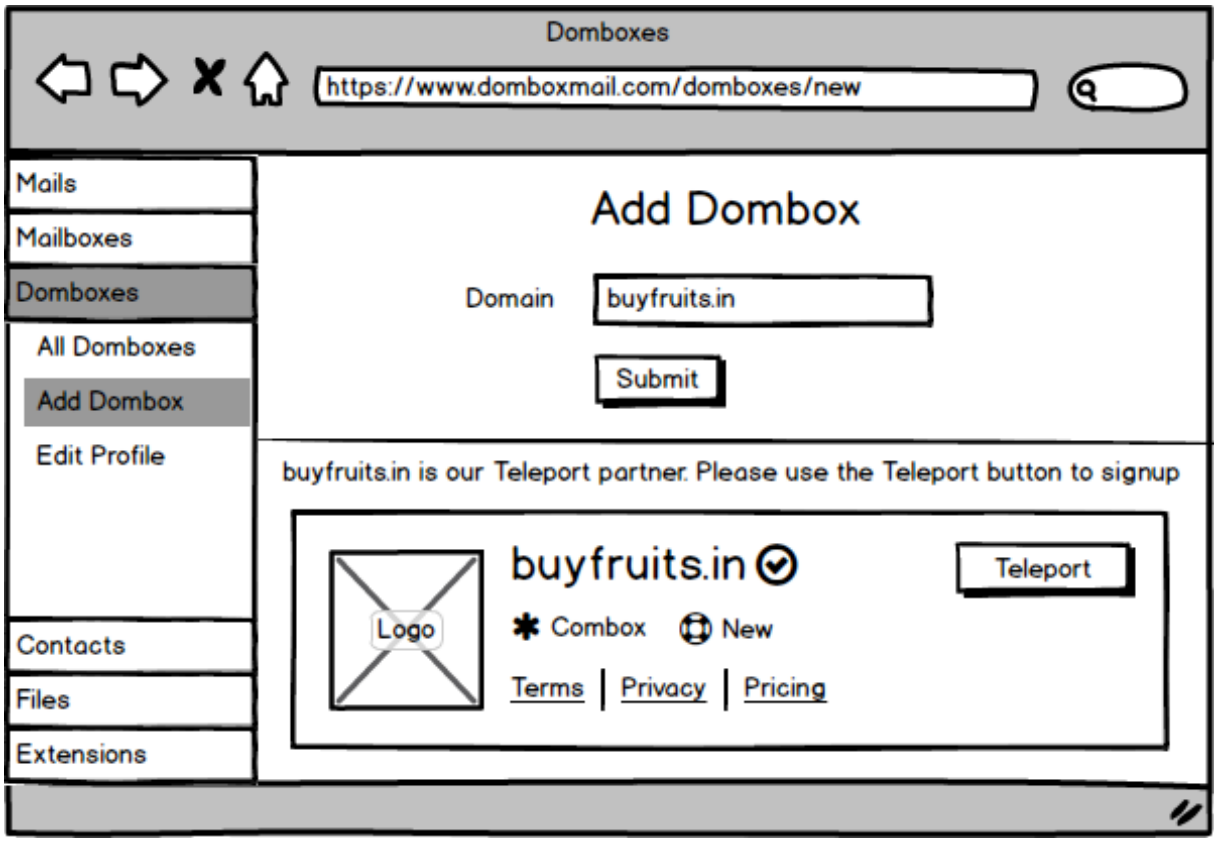


Figure 70: Partner Notice

So “Dombox (D)” box type is disabled for the “Portal Partner” domains.

If you remove the “Teleport” from your website, you are creating a deadlock since we already disabled the Dombox (D) box type. So make sure you are not breaching our “Partner” terms. Otherwise, all your existing contract will be terminated.

Terminating all your contracts will be the final straw. We will keep in touch with you via email if there is an issue.

Note: Don’t get us wrong. You are welcome to remove our “Teleport” button as long as you don’t allow signup / Login via any other methods. e.g. Signup Forms, Facebook connect, Google connect etc.

If you allow only “Login” via other methods, then we expect you to put the “Portal” in

"Login Only" mode. This way we don't allow new contracts, but our existing users can use your website without any issues.

From the "Teleport" button perspective, we consider those websites and apps that supports our "Teleport" button as being part of our "Parallel Internet". Again... That's because our "Parallel Internet" revolves around "i-mail address / Isolated Mailboxes" as opposed to traditional "e-mail address / Normal Mailboxes". So we are expecting the same thing what the "Traditional Internet / Normal Mailbox" Users get from you.

So In simple words, we are looking for "Equal Treatment". In complex legal terms, this is called Most Favoured Nation (MFN)[69] Clause. Although the term "Most Favoured Nation (MFN)" may sound like giving special treatment to a particular nation, it's actually about Non-Discrimination

Termination

Contracts may get terminated in one of the following conditions.

(a) if the business breaches the "Partner" terms and conditions. e.g. Deadlock

(b) if the business is not in "Good Standing" status

(c) If the contract gets automatically expired.

(d) If the user is banned/deleted either by our website or the business website

(e) If the user's account becomes inactive. e.g. User has not logged in for 10 years

When a contract gets terminated, the box will be downgraded from "Combox" to "Hybrid".

Note: When a contract get terminated it only means, the user gets the freedom to delete the box whenever they want. It doesn't mean your business lost a customer.

Portal ID & Secret

Once a Portal created, you can copy Portal ID and Portal Secret. The following example uses the domain "buyfruits.in"

[69] https://en.wikipedia.org/wiki/Most_favoured_nation

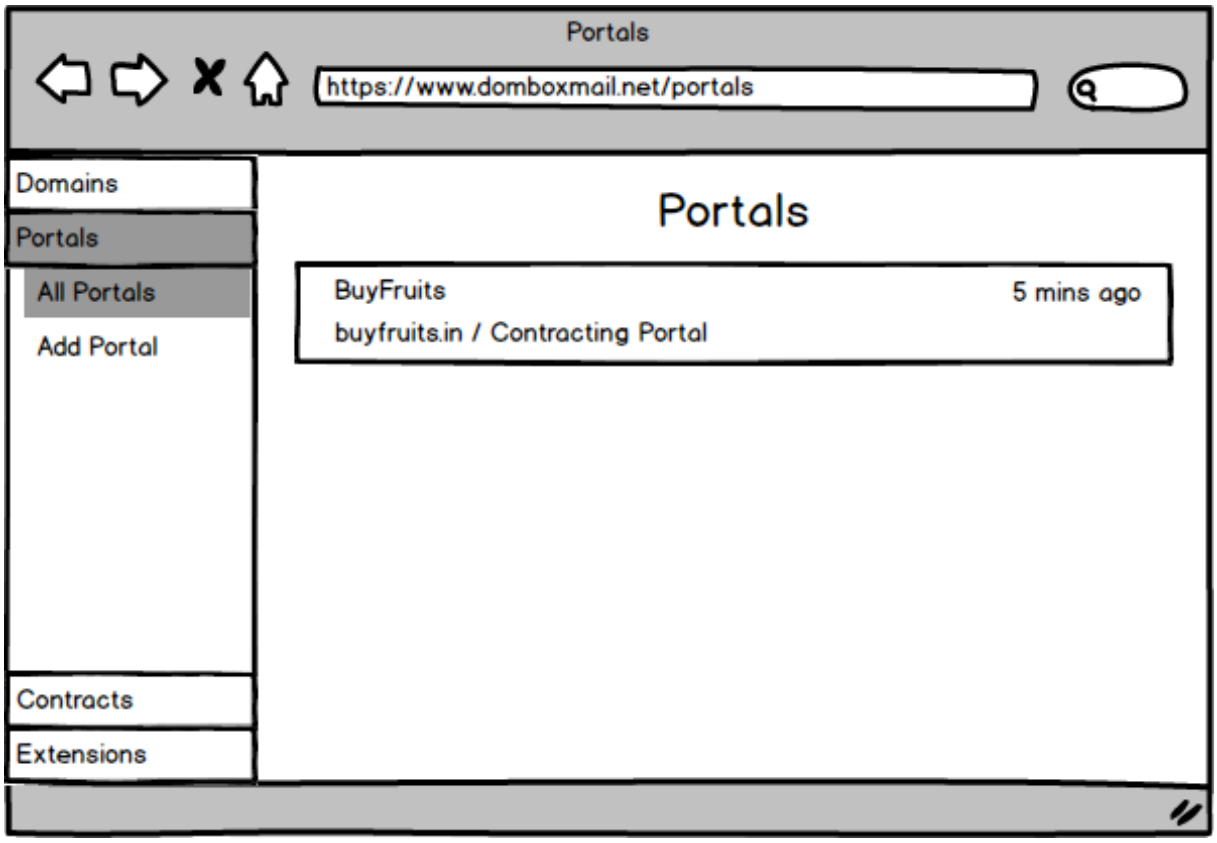


Figure 71: All Portals

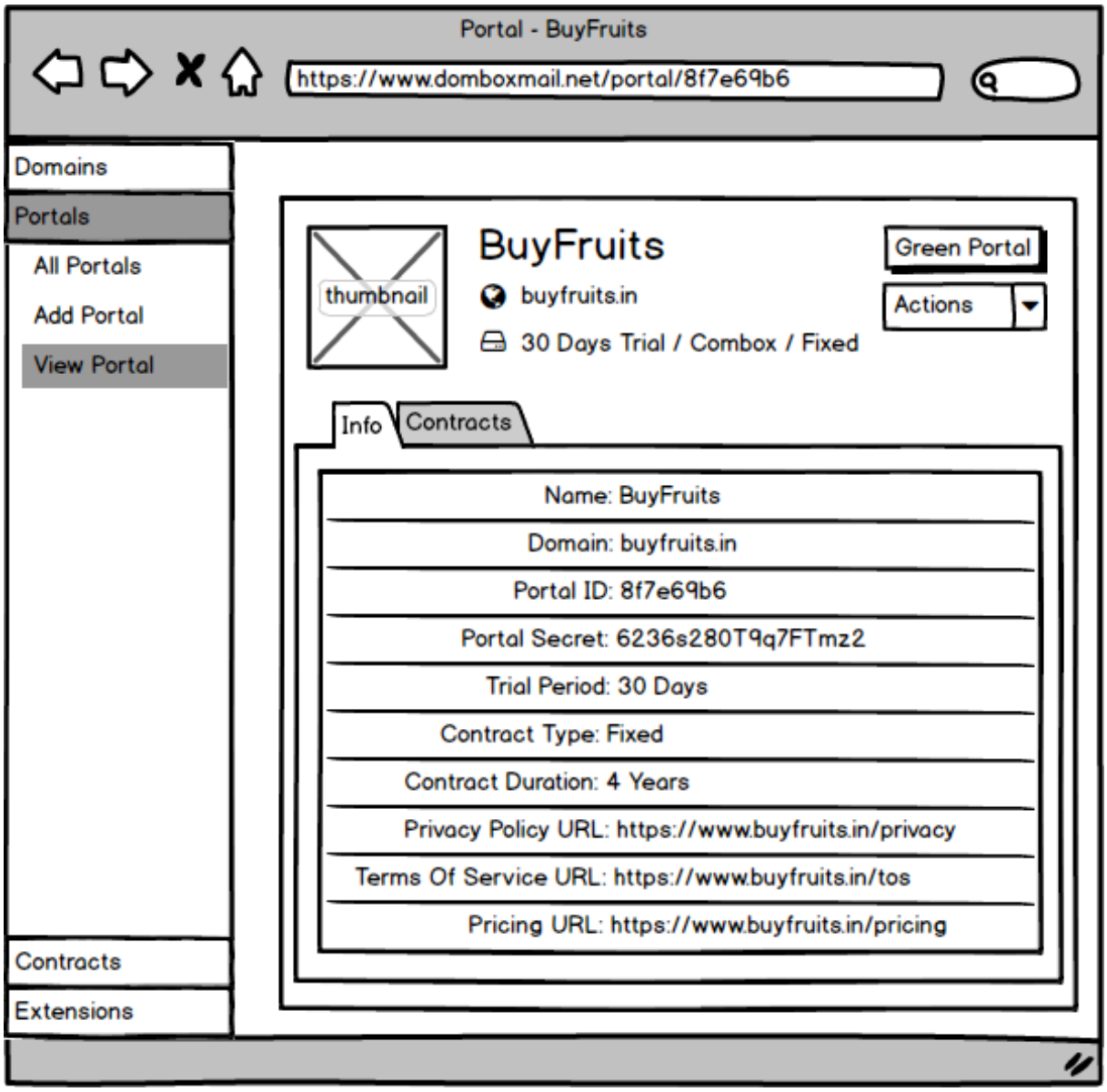


Figure 72: Copy Portal ID and Secret

Copy the “Portal ID” and “Portal Secret” you got from the last image

Go to your website buyfruits.in and then paste it in the portal client (We will be providing the portal client libraries for all programming languages in the future)

Configure Portal

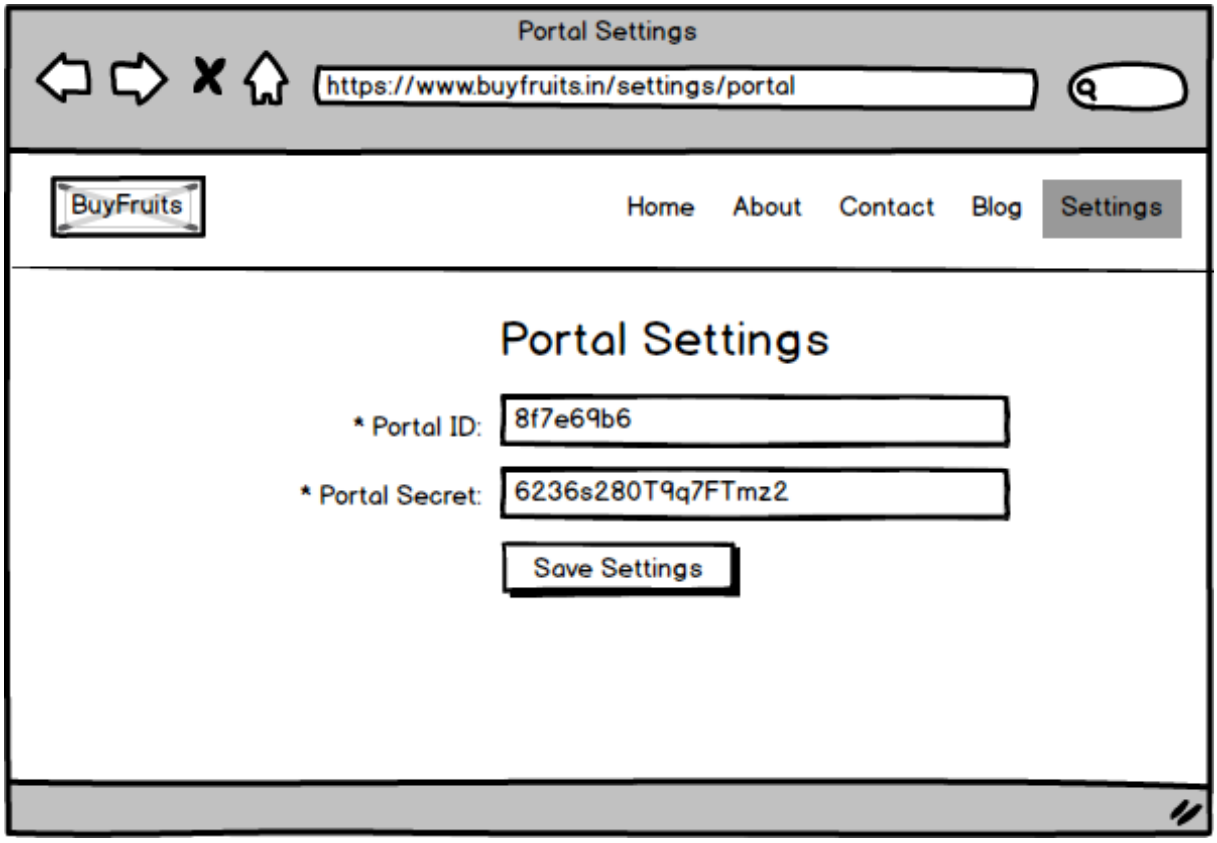


Figure 73: Portal Settings Page on a Portal Partner website

Congrats...

You just created and configured your portal app successfully.

Now... bring some customers to your website.

If any consumer clicks the “Teleport” button from your website that would initiate the “Teleportation” process.

Teleport Process

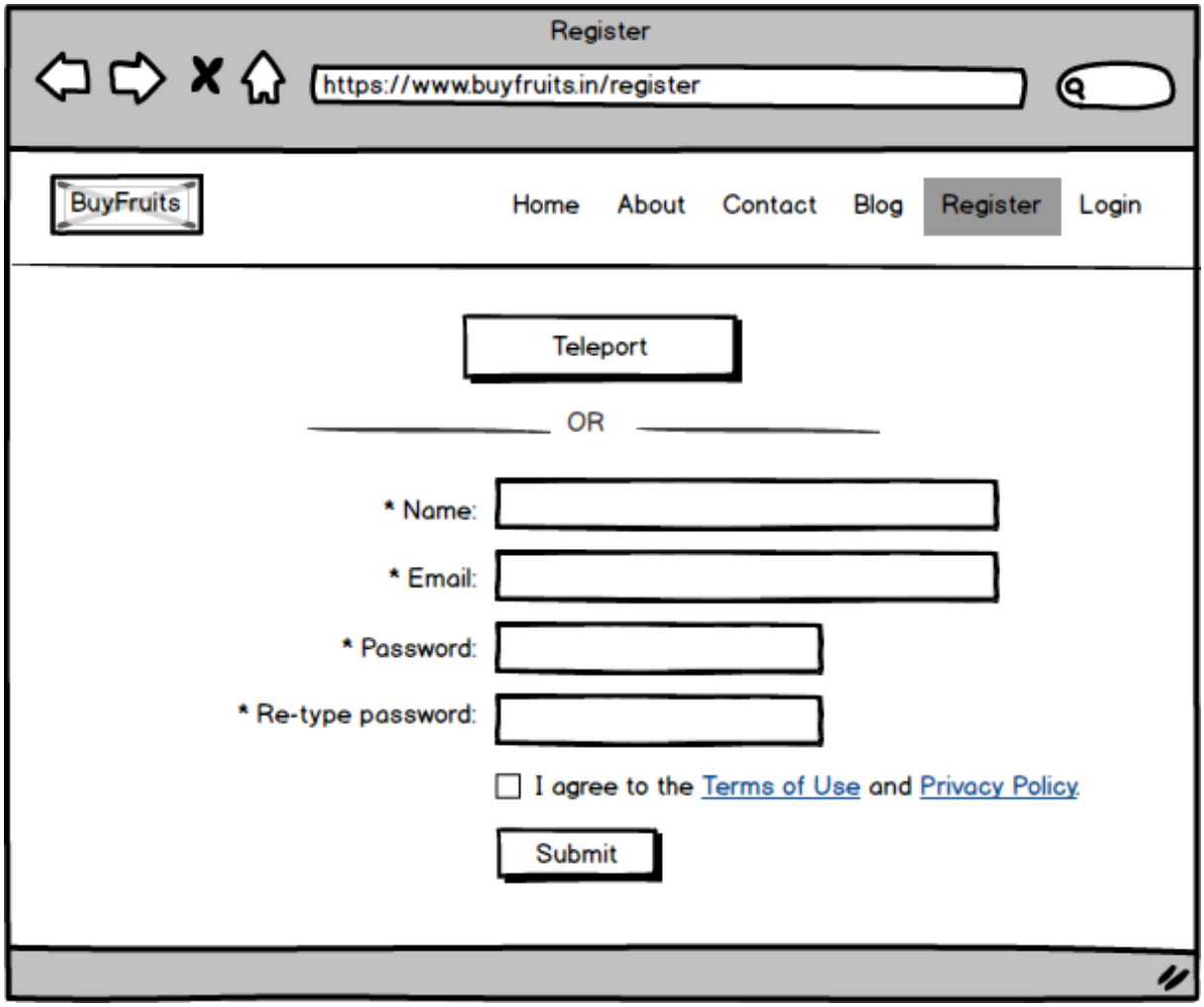


Figure 74: Teleport button on a Portal Partner website

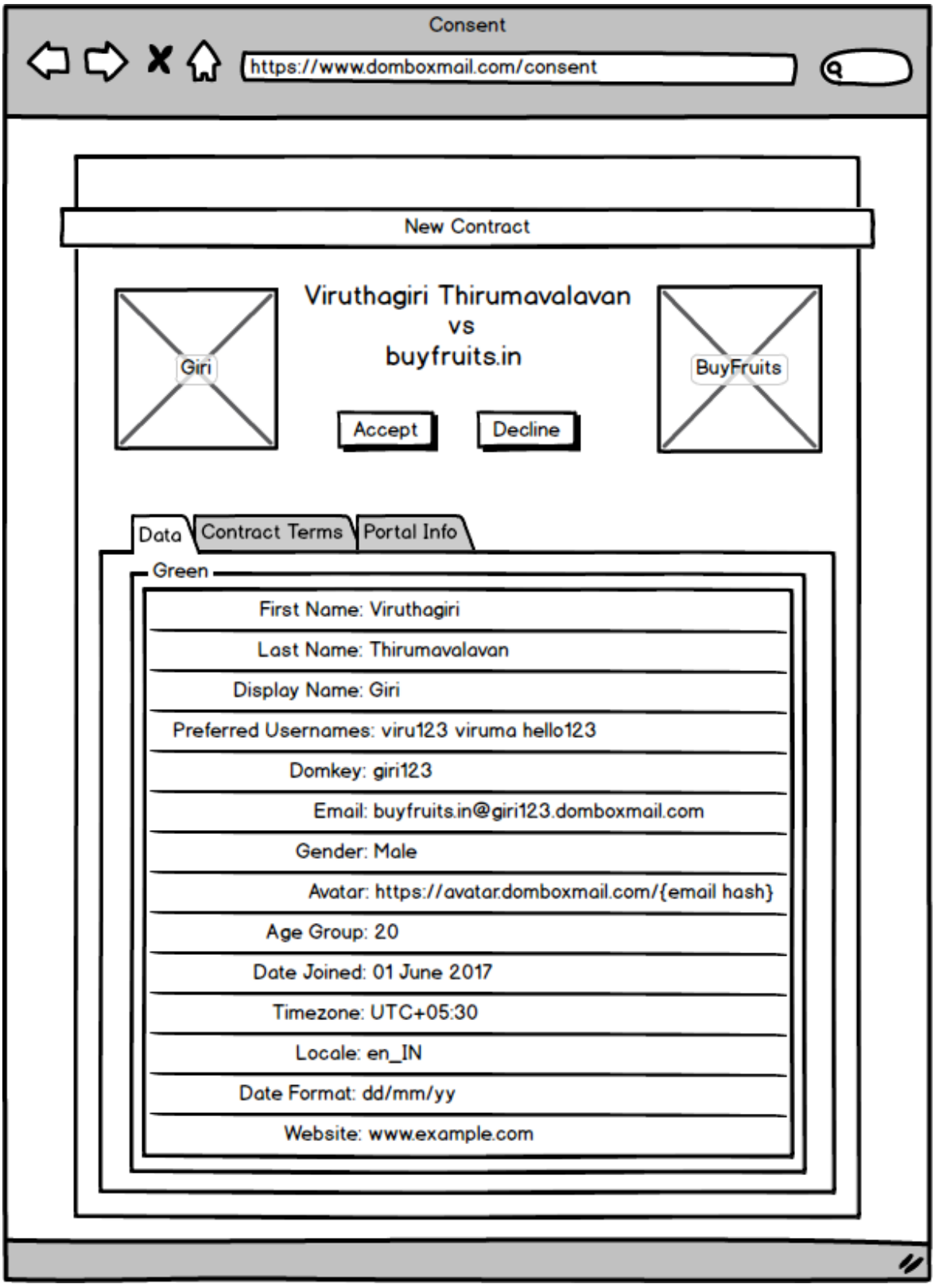


Figure 75: Consent Screen

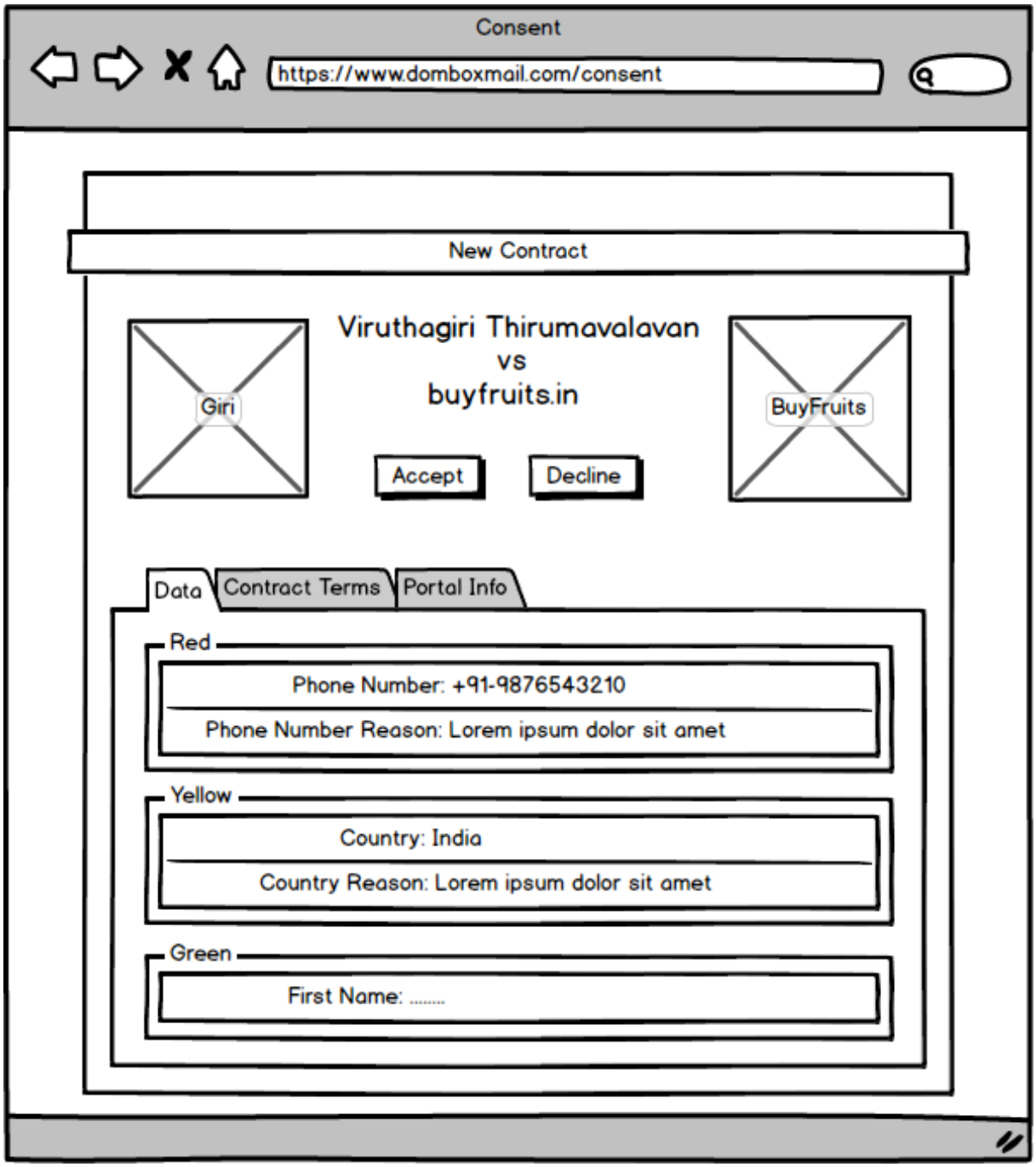


Figure 76: Alternative view when Red & Yellow Data Requested

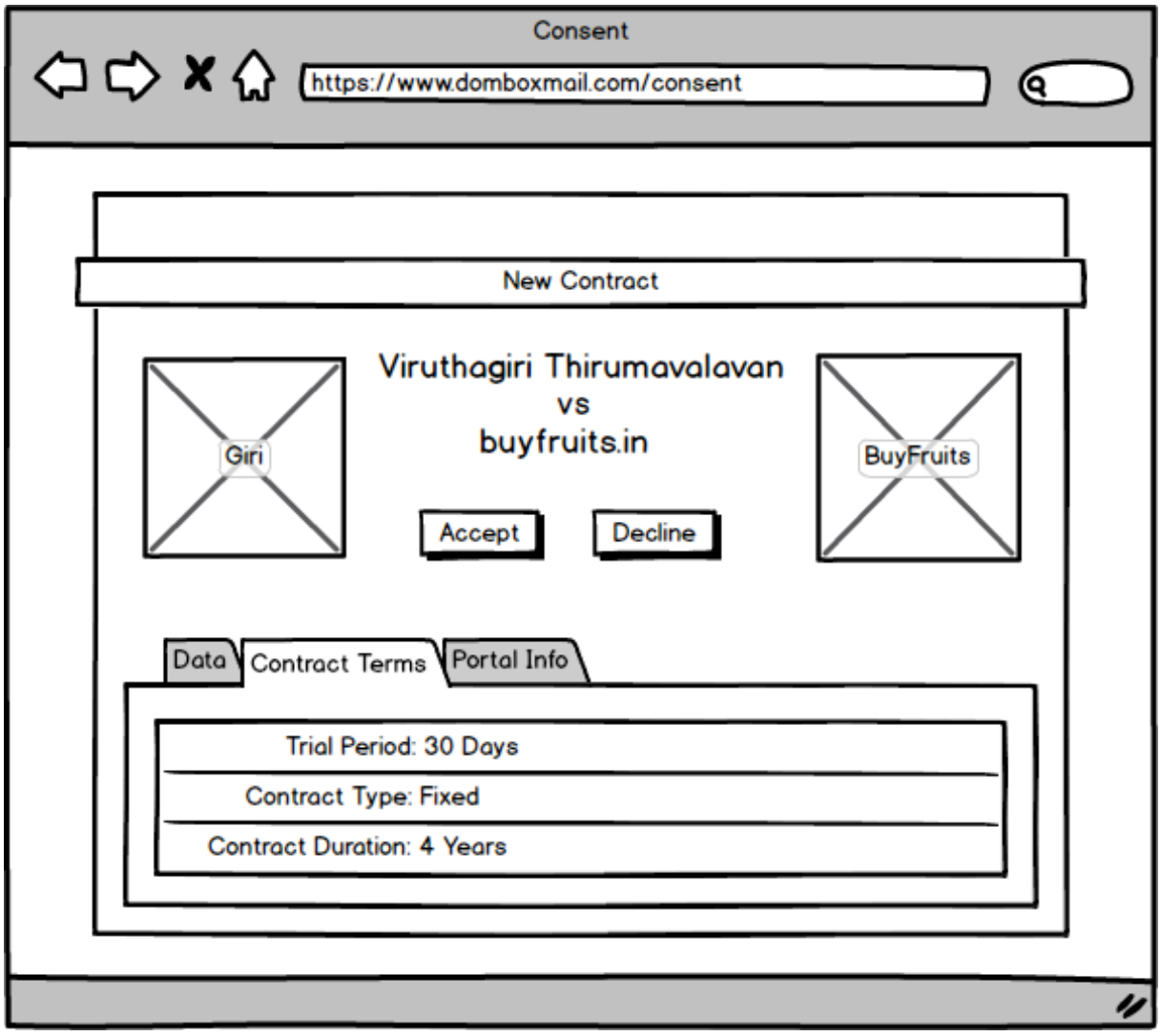


Figure 77: Relative Fixed Contract Terms

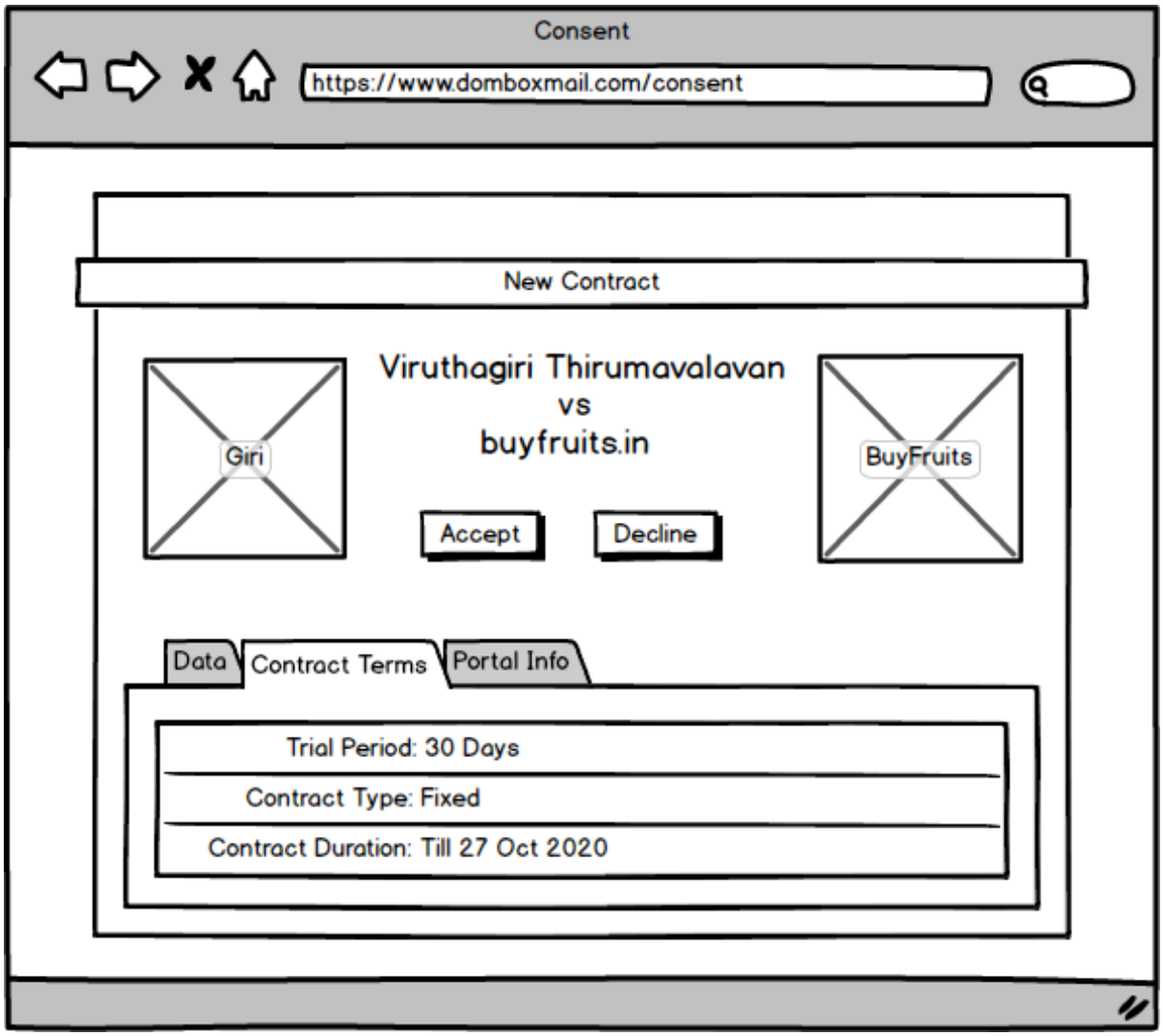


Figure 78: Absolute Fixed Contract Terms

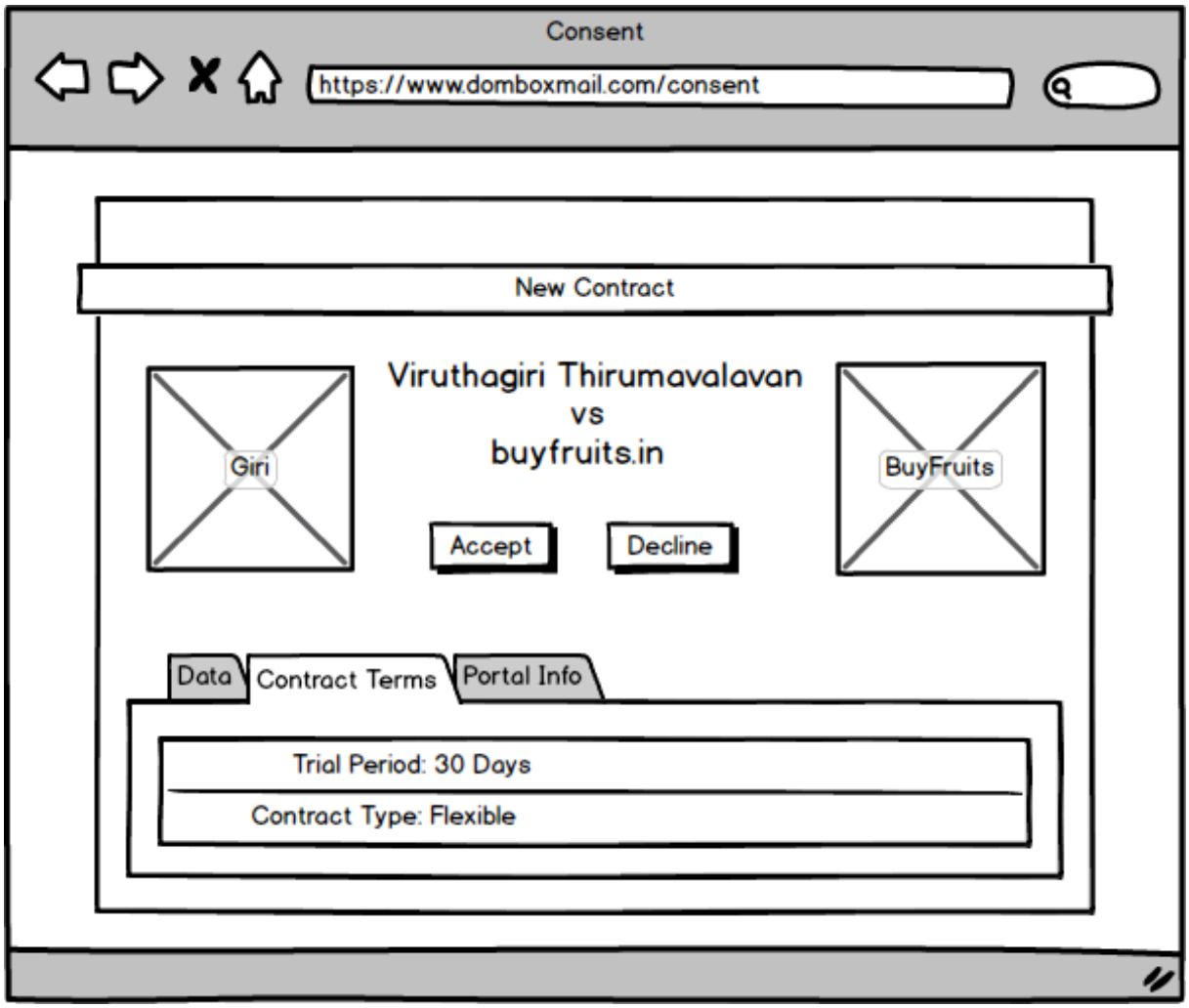


Figure 79: Flexible Contract Terms

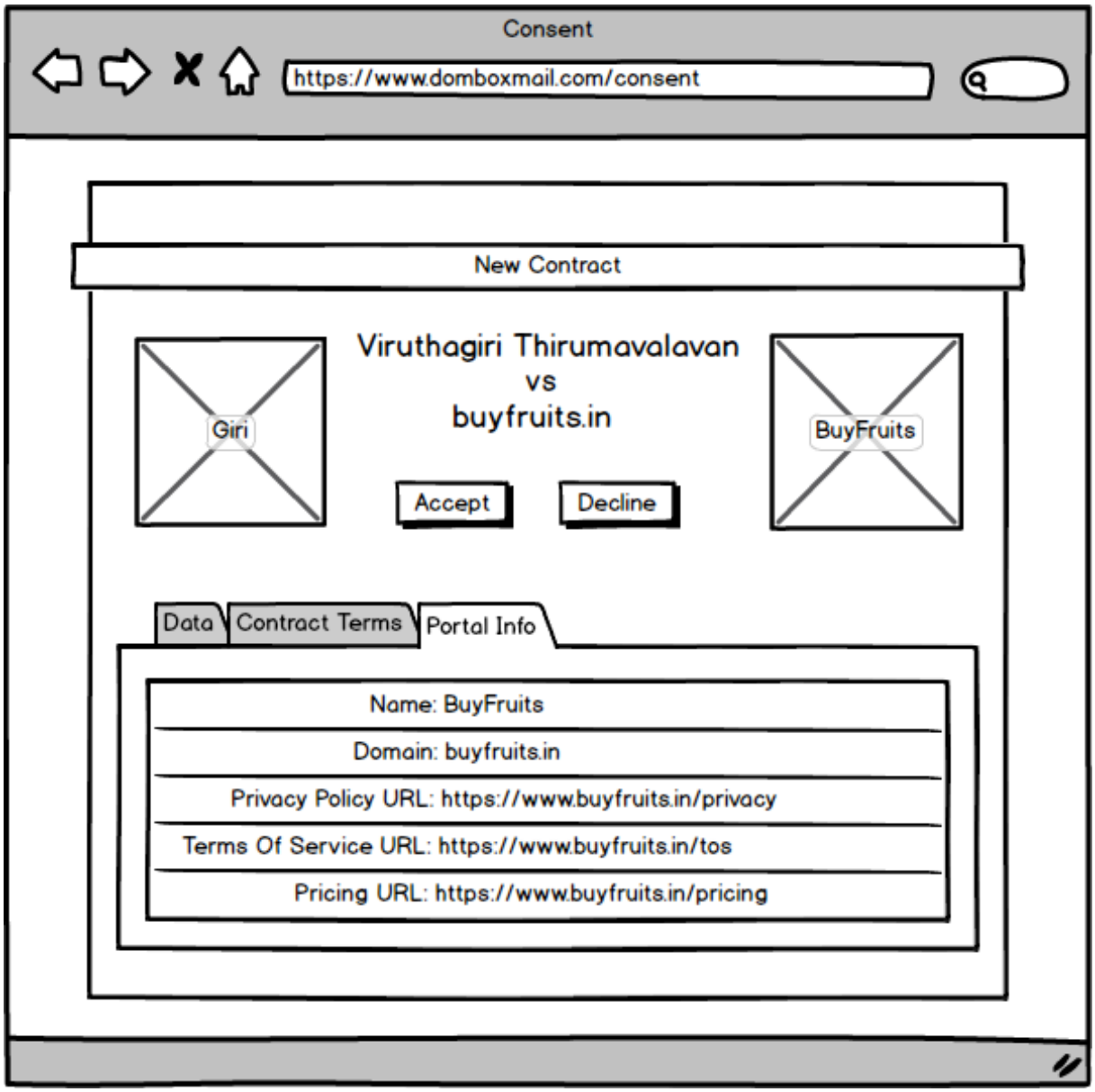


Figure 80: Portal Info

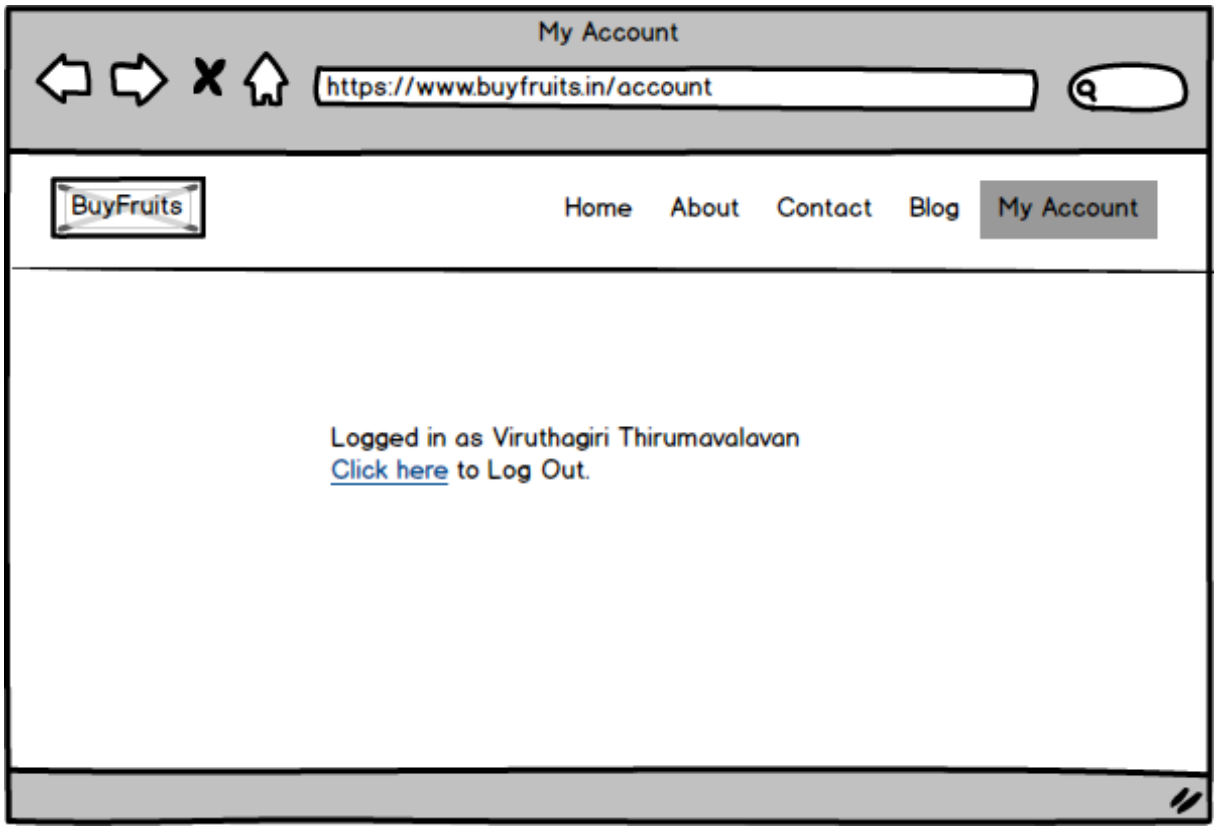


Figure 81: Successful Signup via Teleport

Combox via Teleport

The next two images illustrate the Combox created via Teleport button

The next two images represents the “consumer” side.

Combox (C) Box Type doesn’t have the “Make Offline” and “Delete” Options.

So Combox will always be “Online”

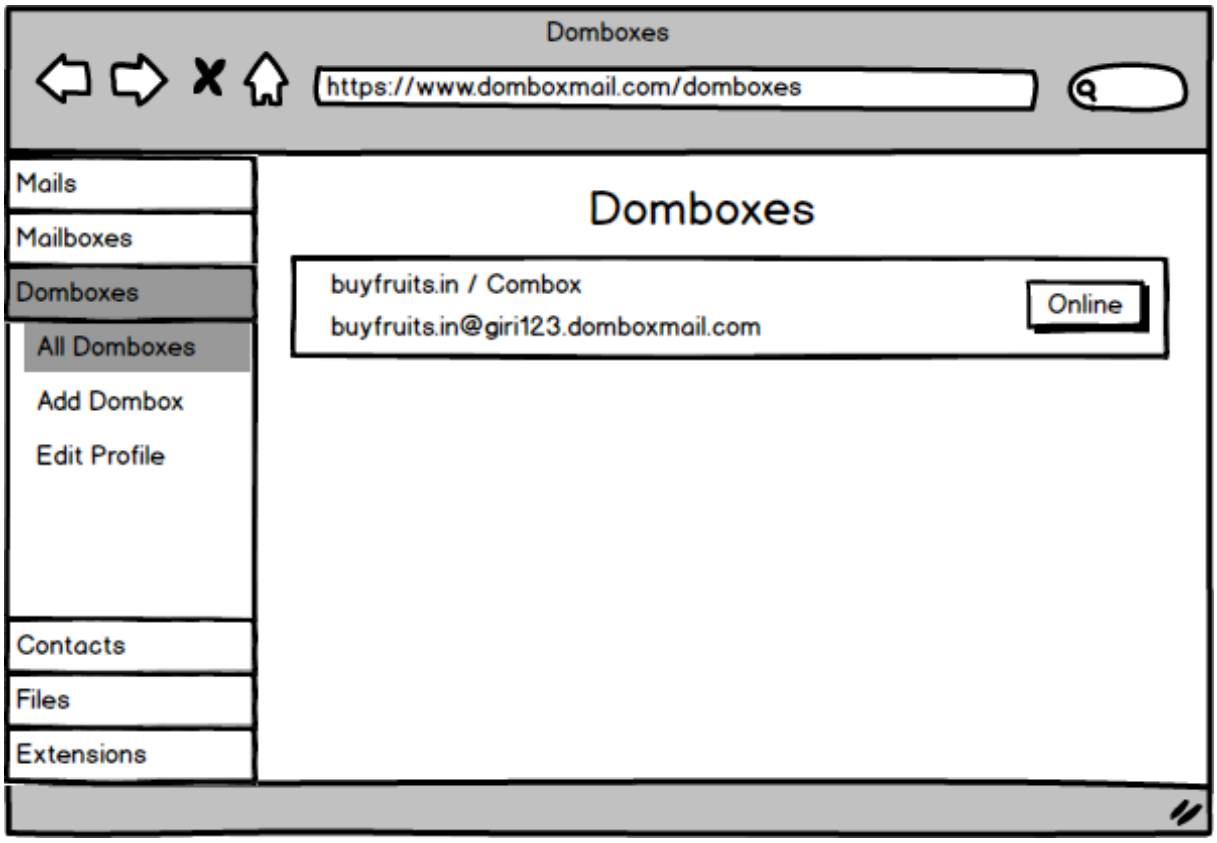


Figure 82: Combox on Domboxes page

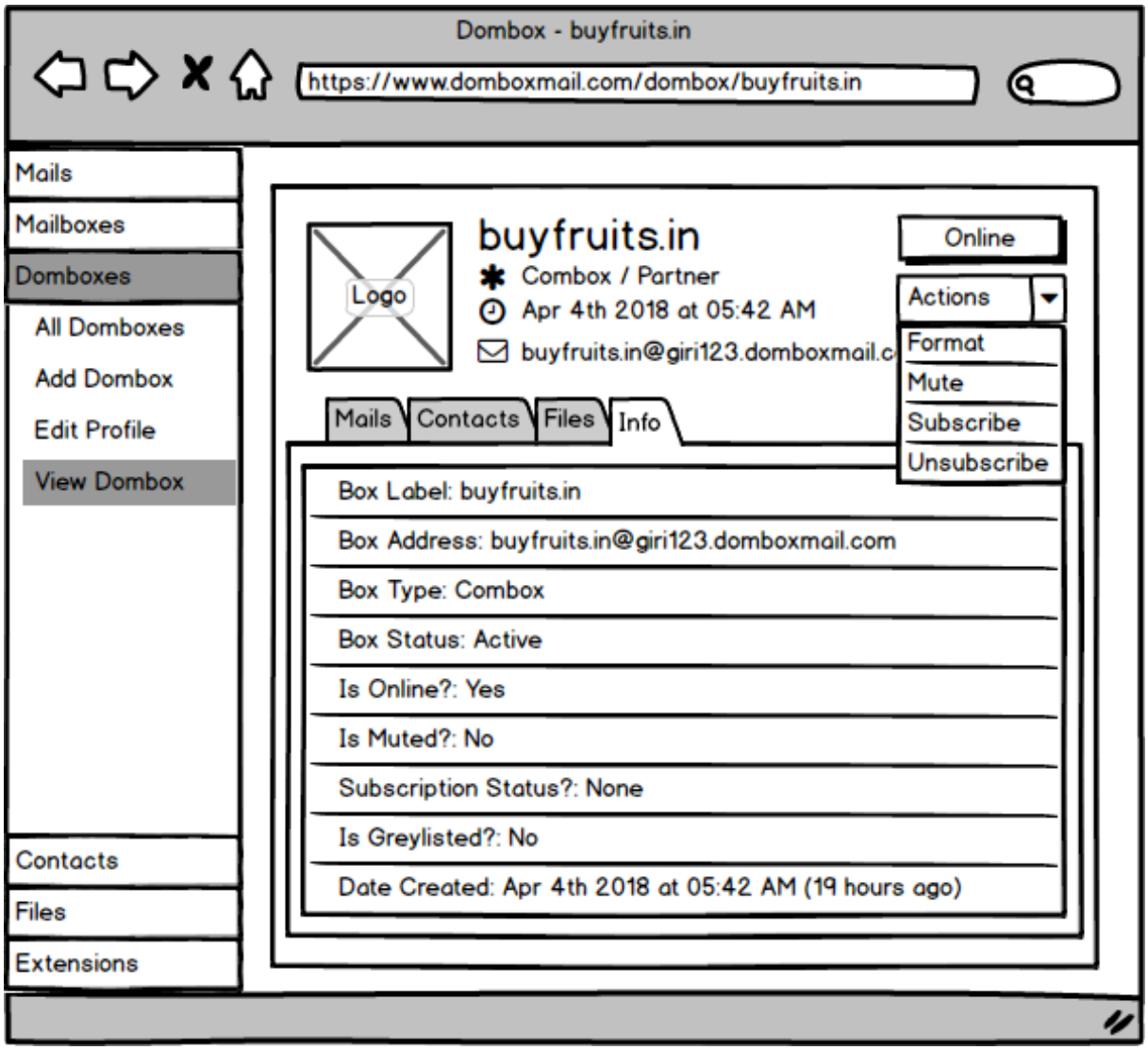


Figure 83: Combox Info

Contract via Teleport

The next few images illustrate the Contract created via Teleport button

The next few images applicable only for website owners

The contract can be viewed by the website owner from the dashboard

All contracts are available under the “Contracts” menu. This page lists the contracts from all Portals

Contracts related to a particular “Portal” can be browsed from the “View Portal” page

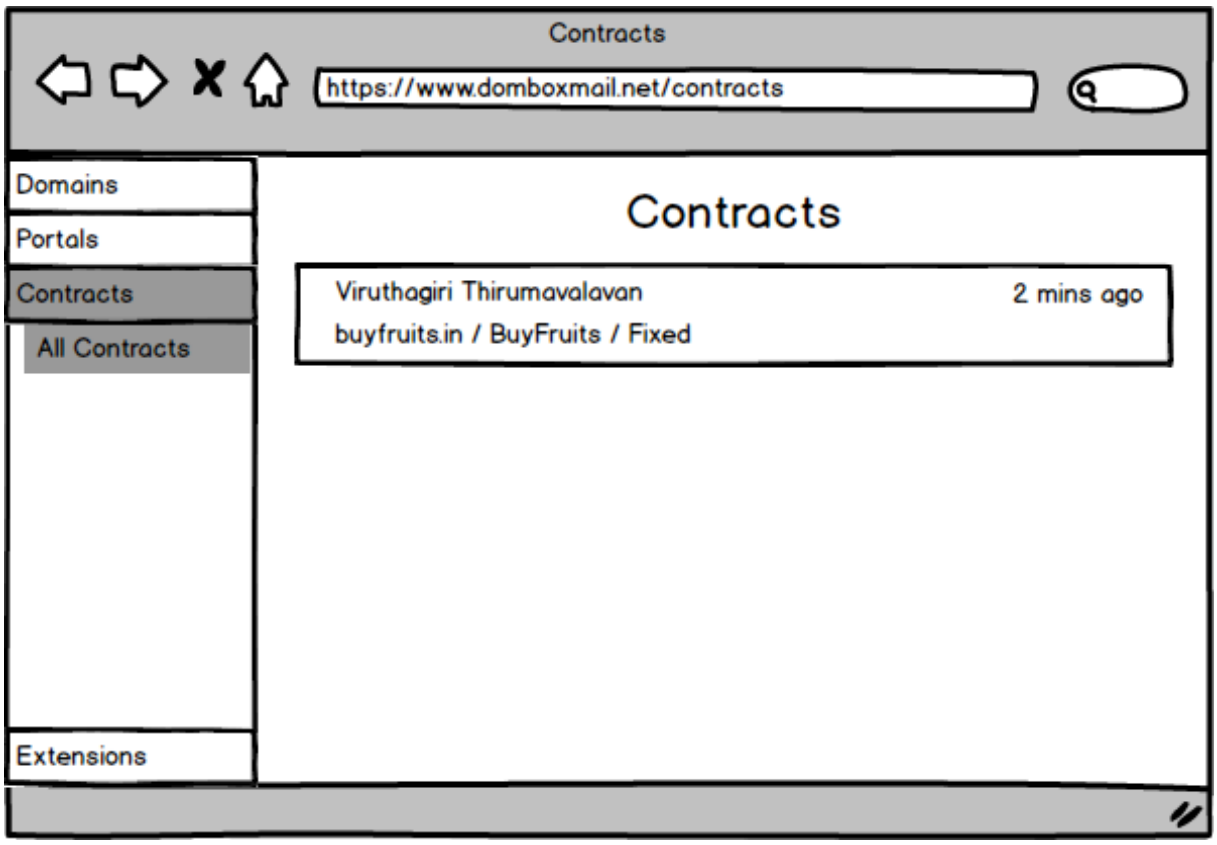


Figure 84: Contract created via Teleport

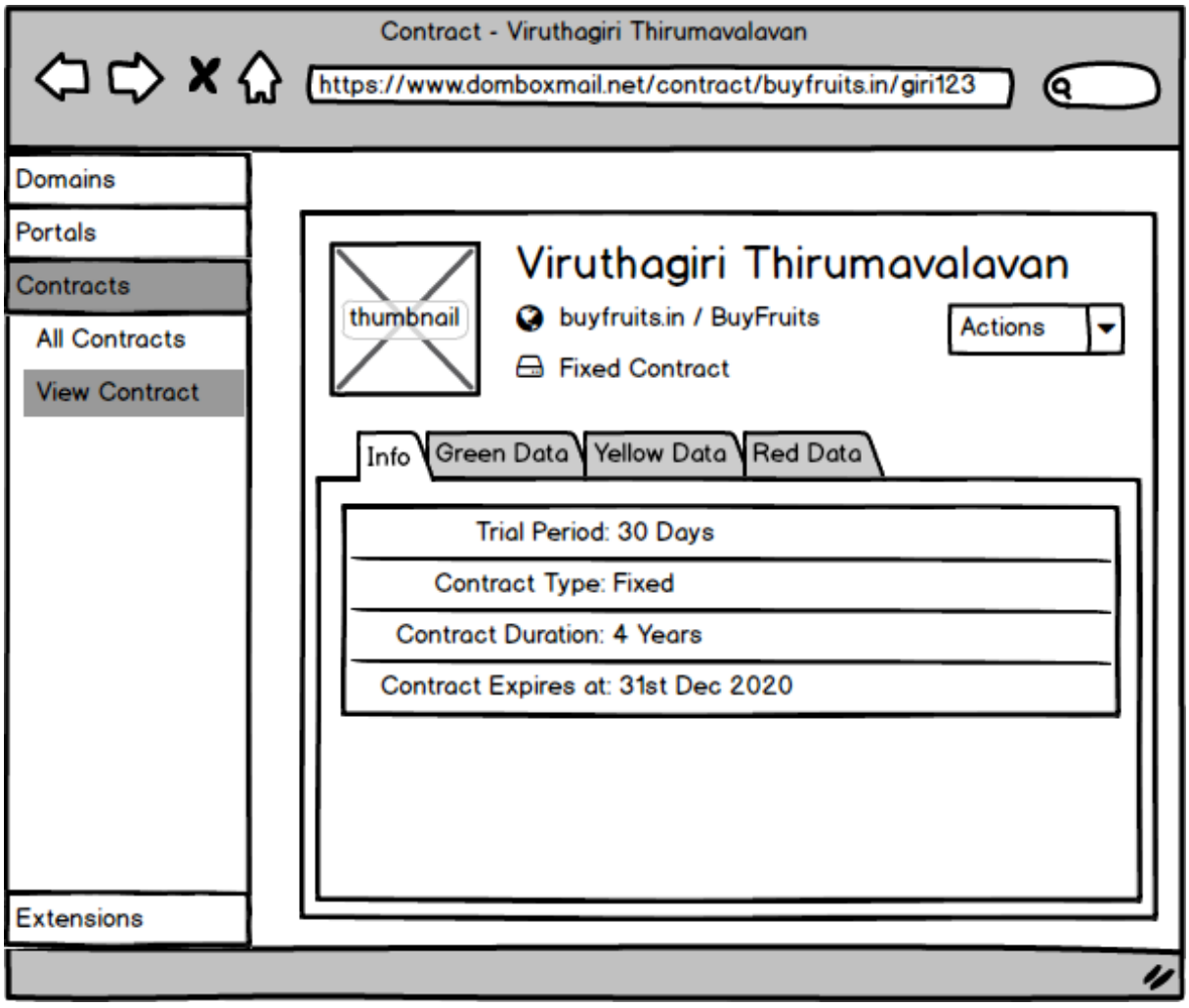


Figure 85: Contract Info

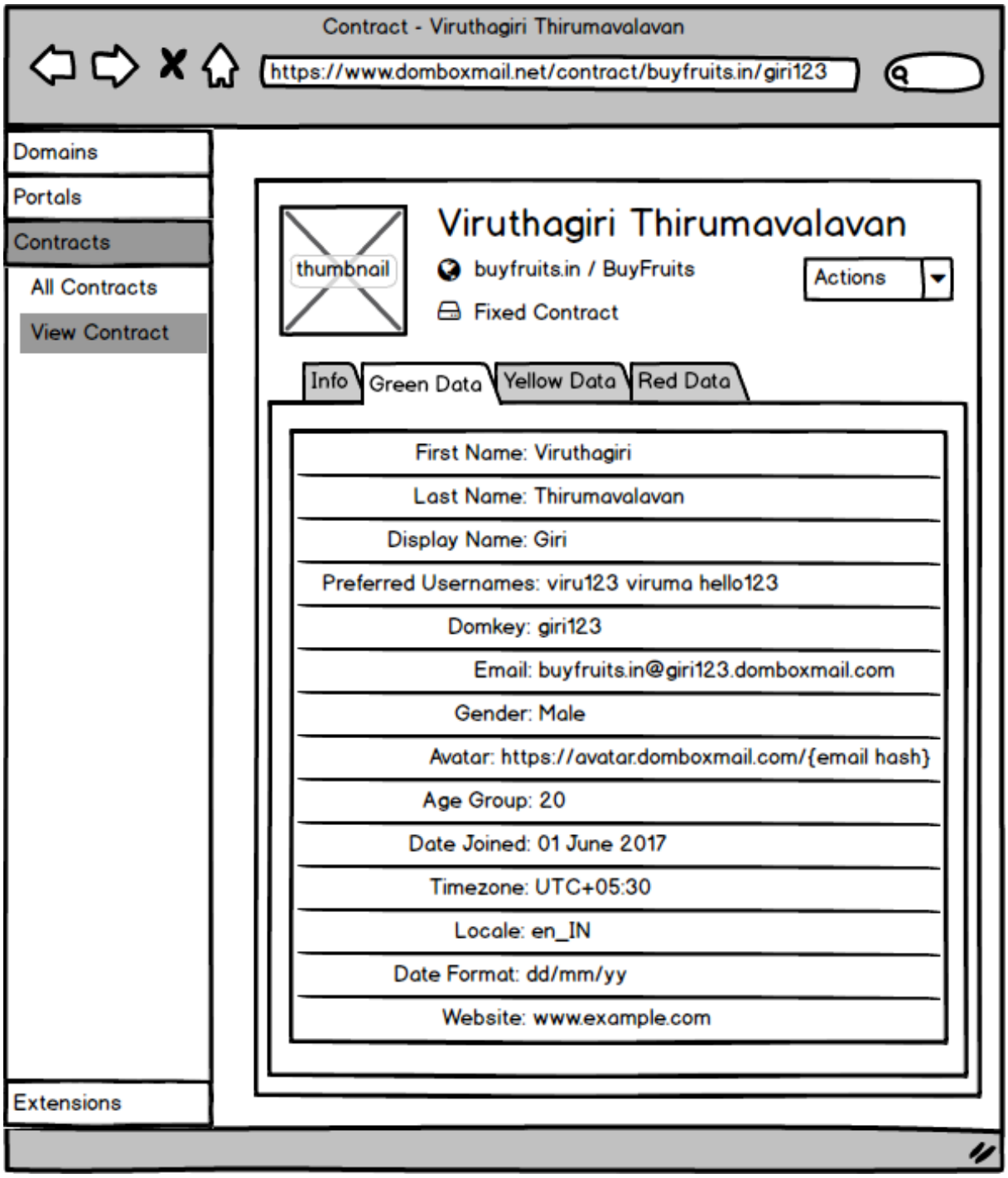


Figure 86: Contract - Green Data

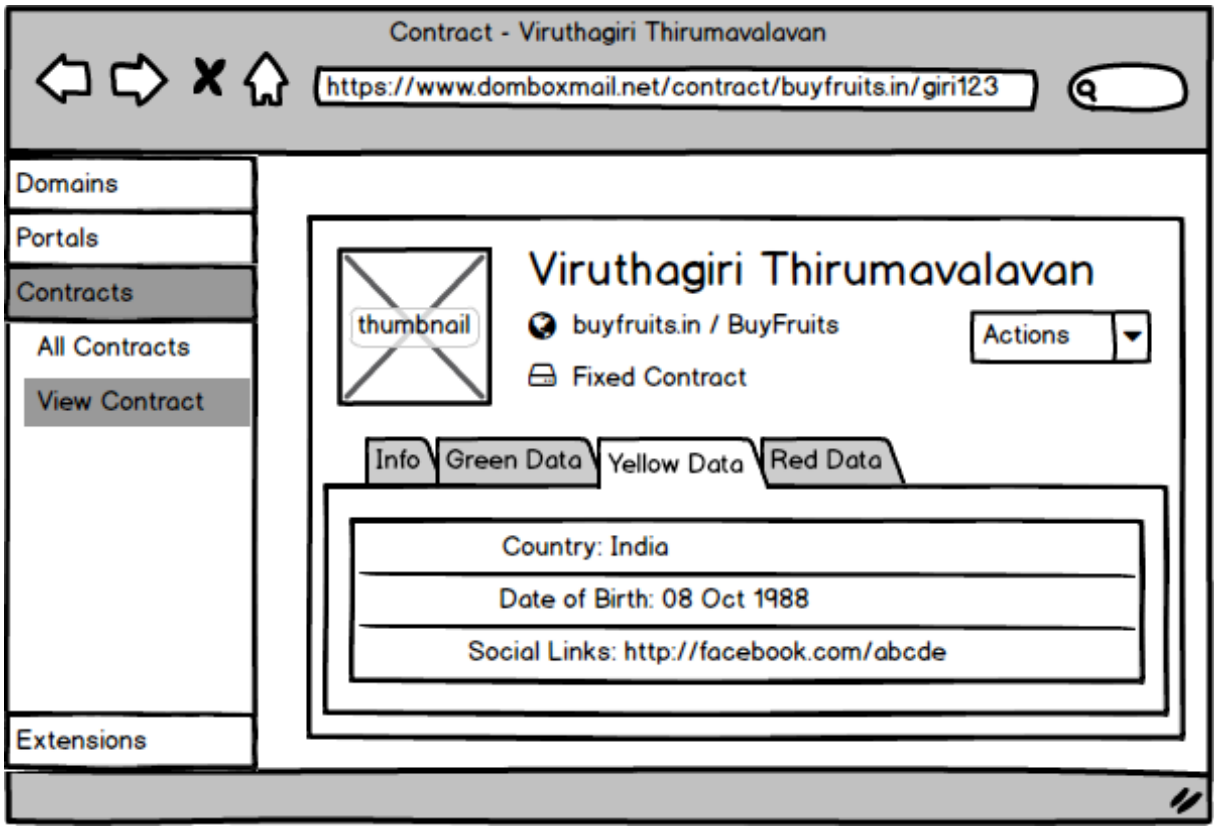


Figure 87: Contract - Yellow Data

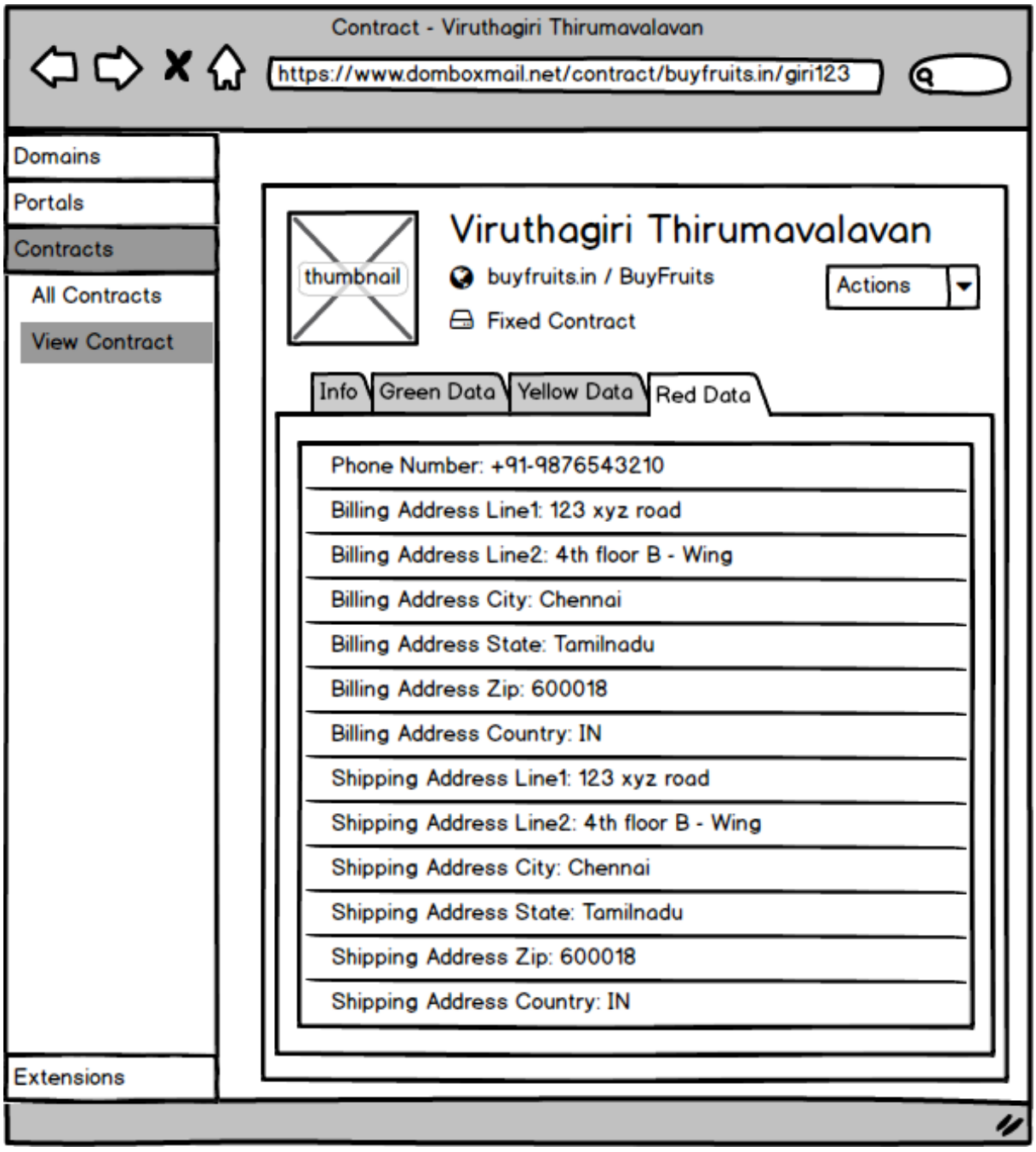


Figure 88: Contract - Red Data

Partner Policies

When a domain become our portal partner, they need to comply with certain policies. If they don't comply, then they may lose the contracts.

Fair Mailing Policy

In our system, we classify the mails into three categories. Conversational Mails, Transactional Mails and Promotional Mails.

If you are Amazon, all your customer support mails are falling under the "Conversational Mails" category. All purchase receipts are falling under the "Transactional Mails" category. We have no restriction on the Conversational Mails and Transactional Mails.

But for "Promotional Mails", you must respect the user's subscription preference. If a user is unsubscribed, it means the user is not interested in receiving any "Promotional Mails" from you.

However, you can send them "News-Letters" anytime you want.

HeadsUp! It's "News-Letters". Not "Newsletters".

News-Letters

The term "Newsletter" heavily misused these days. Sometimes, when you click a random link found in the Google search results, you will get a popup saying "Subscribe to our Newsletter".

Once you Opt-In, you are gonna get non-stop mails from that website. And then you will be like "Leave me alone", "Please I beg you, get me off from your list" etc.

We are not talking about that kind of "Newsletters" here.

In our terminology, The term "News-Letters" refers to "Newsworthy-Letters". Pay attention to the "Hyphen".

So, the real question is "What exactly is a Newsworthy-Letter?"

Well… That depends on your industry. If your news can be termed as “big news”, “breaking news” etc. by your recipients, then those mails are definitely falling under “Newsworthy-Letters” category. e.g. We have been acquired by Microsoft, We have been Hacked, We introduced a new product etc.

You are about to send this mail to all your users even to the people who unsubscribed. You don’t want to annoy them. So just ask yourself this question.

If I were a Journalist in “[insert a well respected magazine name in your industry]”, would I report the news “[insert your mail subject here]” to the readers?

Examples:

If I were a Journalist in “Techcrunch”, would I report the news “We have been acquired by Microsoft” to the readers?

If I were a Journalist in “Techcrunch”, would I report the news “20 reasons why our product is awesome” to the readers?

Styling:

Correct => news-letter, News-Letter, news-letters, News-Letters

Incorrect => News-letter, News-letters, News_Letters

If you see a newsletter form with title like “Subscribe to our News-Letter” somewhere in the future on a non portal partner website, then they are talking about our “Newsworthy-Letters”. You are going to get only important news from them.

Fair Migration Policy

We have a “Fair Migration Policy” where you can rename the Combox mail address without consumer permission.

However, you still need to notify the users about the domain change.

For example, The consumer signed the contract on example.com and you would like to rename the domain to example.net. This would fall under our fair migration policy.

giri123$example.com@domboxmail.com => giri123$example.net@domboxmail.com

test123$example.com@domboxmail.com => test123$example.net@domboxmail.com

hello123$example.com@domboxmail.com => hello123$example.net@domboxmail.com

But you cannot migrate a domain, contrary to its name.

Consumer signed up to ILoveDonaldTrump.com. You cannot rename it to IHate-DonaldTrump.com

Also, there will be a limitation in the migration feature. This is because we don't want the website owners to keep on renaming their domains.

Note: If you pivot your product to something else with a completely irrelevant domain, you cannot use our "Fair Migration" feature. You have to either ask your users to signup to your new product OR add a SAD record in your old domain by whitelisting the new domain. If you are going for the latter option, never lose access to your old domain.

Chapter 11: Data

User Data is classified into three categories.

Data	Sensitivity
Green Data	Low
Yellow Data	Medium
Red Data	High

Data access is a three-step process

Player	Action
Consumers	Fills their personal data by editing the profile
Business Owners	Request Consumer Data via Portal

Player	Action
Consumers	Give permission to business to access their data via “Teleport”

Green Data

If a third party website gets hacked, the damage is nearly null in this category. This is because all data found in this category are Insensitive ones (including email address).

e.g. Back in 2013, 150 million[70] Adobe accounts were hacked. If Adobe had only our green data, they can contact our consumers without any issues, on the other hand, this data is useless in the spammers hands. Because hacking this data is nothing more than crawling Facebook profiles.

For most websites, only Green Data is enough. If you are a website owner, keep in mind you are discouraging user signups if you request “Yellow Data” and “Red Data” without a sensible reason.

“Green Data” contains the following fields.

First Name, Last Name, Display Name, Preferred Usernames, Domkey, Email, Gender, Avatar, Age Group, Date Joined, Time Zone, Locale, Date Format, Website

Field	Description
First Name	Self-Explanatory
Last Name	Self-Explanatory
Display Name	Display name provided by the Consumer. If provided websites are advised to use this name in profile display instead of consumer’s full name.

[70] https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online

Field	Description
Preferred Usernames	Some websites requires a username to create “Vanity URL”. This is a comma separated value. The website can use the usernames if available
Domkey	Explained already
Email	Isolated Email Address. Not the primary email
Gender	Consumer’s Gender. It can be one of the following values. Male (M), Female (F), Others (O)
Avatar	Avatar URL
Age Group	Consumer’s age group. If the consumer is in his/her twenties, then this value would be 20. If the consumer is in his/her thirties, then this value would be 30 and so on. The possible value would be from 10 to 120
Date Joined	Consumer’s signup date to the Dombox mail service.
TimeZone	Timezone value set by the Consumer. So the website can display date and time based on the consumer’s time zone.
Locale	Preferred Language Locale value set by the Consumer. If the website supports the locale, then the website user interface would use that locale. e.g The value “en_US” means US English. The value “en_GB” means UK English
Date Format	Date format value set by the Consumer. So the website can display date based on the consumer’s date format.
Website	Website value set by the Consumer. So the business can display the website URL in profile if provided.

Yellow Data

If a third party website that contains the yellow data get hacked, then the damage is minimal.

“Yellow Data” contains the following fields.

Date of Birth, Country, Social Links.

Keep in mind, the consumer has the option to decline Yellow Data and Red Data requests.

Yellow Data and Red Data require a valid reason for each field.

For instance, Yellow Data contains “Date Of Birth” field. If some website needs to access that data, then a valid reason is required from them. e.g. “Adult website. For age verification” is a valid reason. But “To send birthday wishes” is not.

Field	Description
Date of Birth	We put the “DOB” field in the “Yellow” category because it requires moderate privacy. e.g. Search results for “Name: John Smith” => 10,000 results. Search results for “Name: John Smith and DOB: 05/05/1985” => 2 results.
Country	We put the “Country” field in the “Yellow” category because it also requires moderate privacy. e.g. Some websites may block users from a certain country. Users usually bypass that by faking the IP address with a “Proxy”. So giving country data to the website in “Green Data” is not a good idea
Social Links	Social Links are put in “Yellow” category because social profiles are prone to stalking.

Red Data

Red Data contains highly sensitive fields. Phone Number, Billing Address, Shipping Address

These data will be helpful when signing up for e-commerce websites

Again.. the consumer has the option to decline the Red Data request.

And Red Data requires a valid reason for each field.

A portal that requests access for at least one “Red Data” field is called “Red Portal”

A portal that requests access for at least one “Yellow Data” data but not “Red Data” fields is called “Yellow Portal”

A portal that requests access for only “Green Data” fields is called “Green Portal”. By default, all portals have full access to this data.

Consumer Side

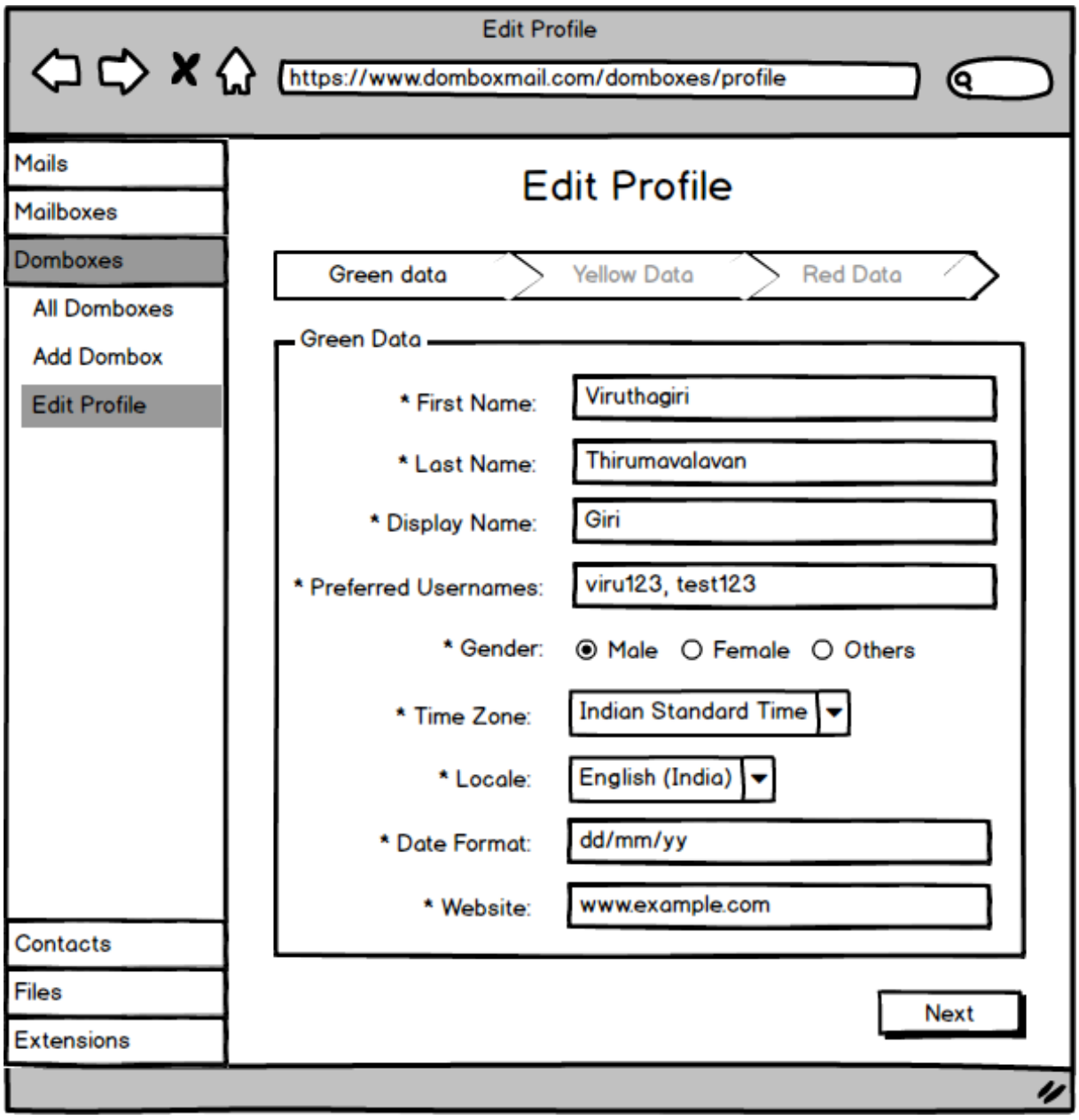


Figure 89: Consumer Side - Green Data

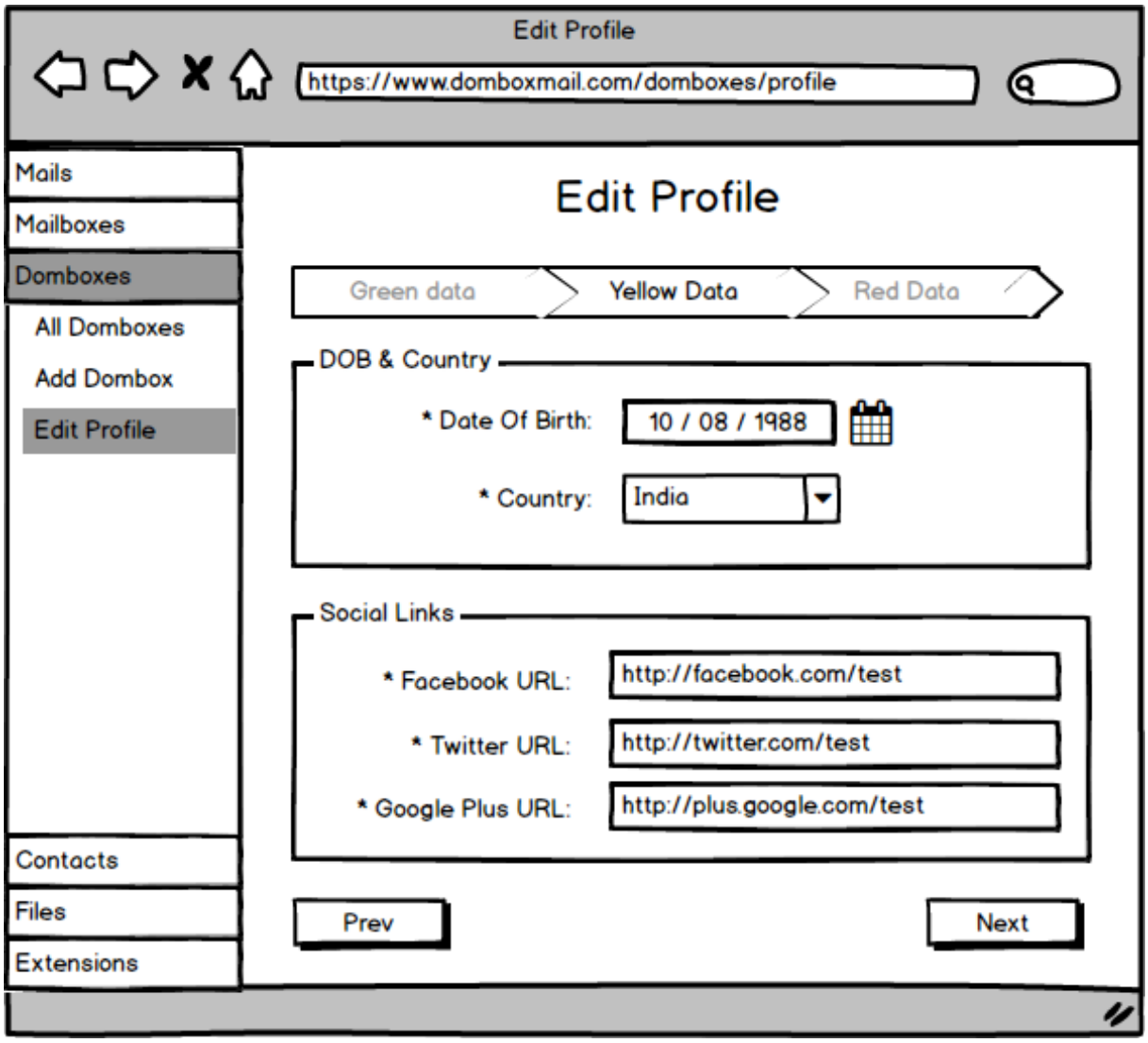


Figure 90: Consumer Side - Yellow Data

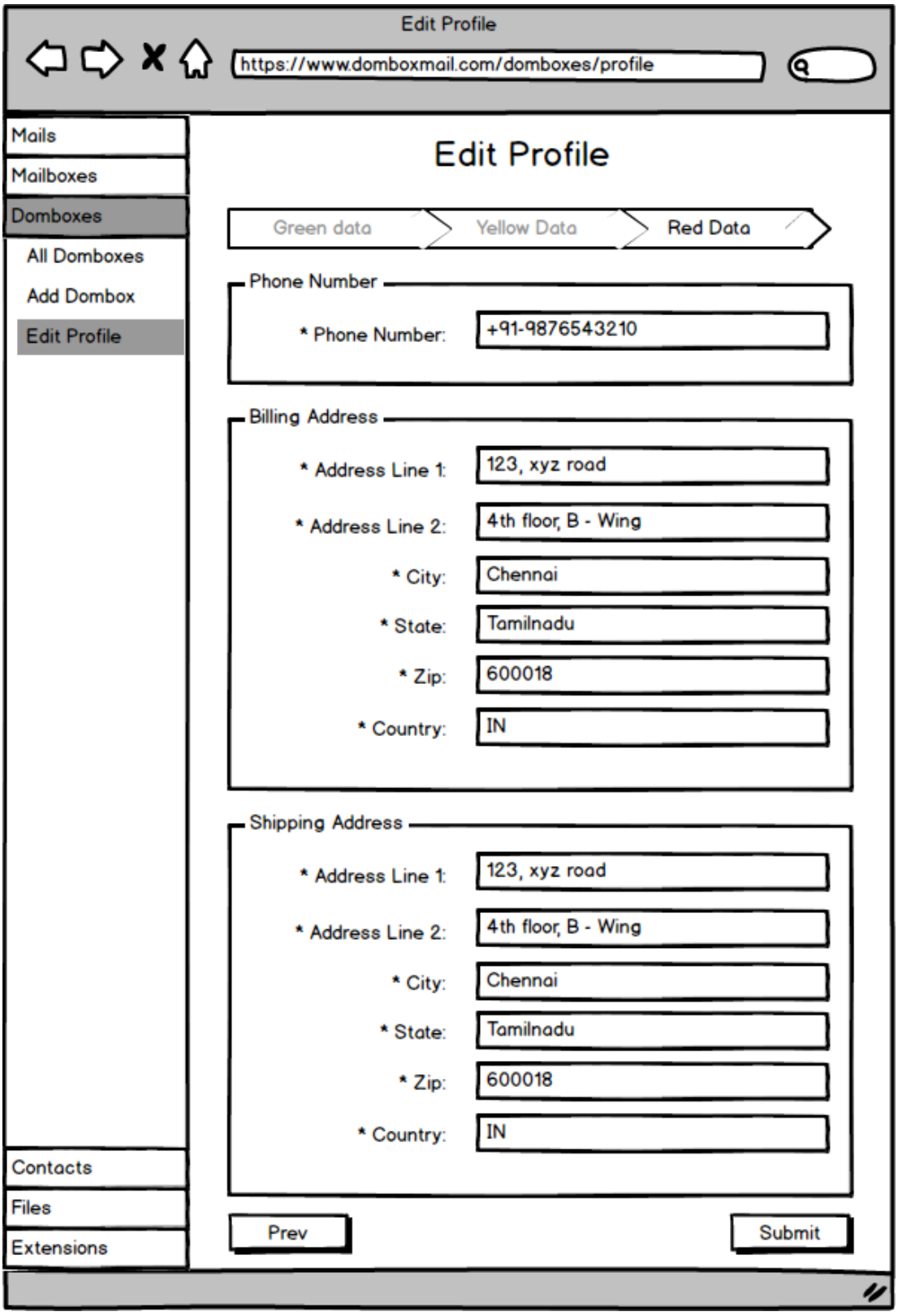


Figure 91: Consumer Side - Red Data

Business Side

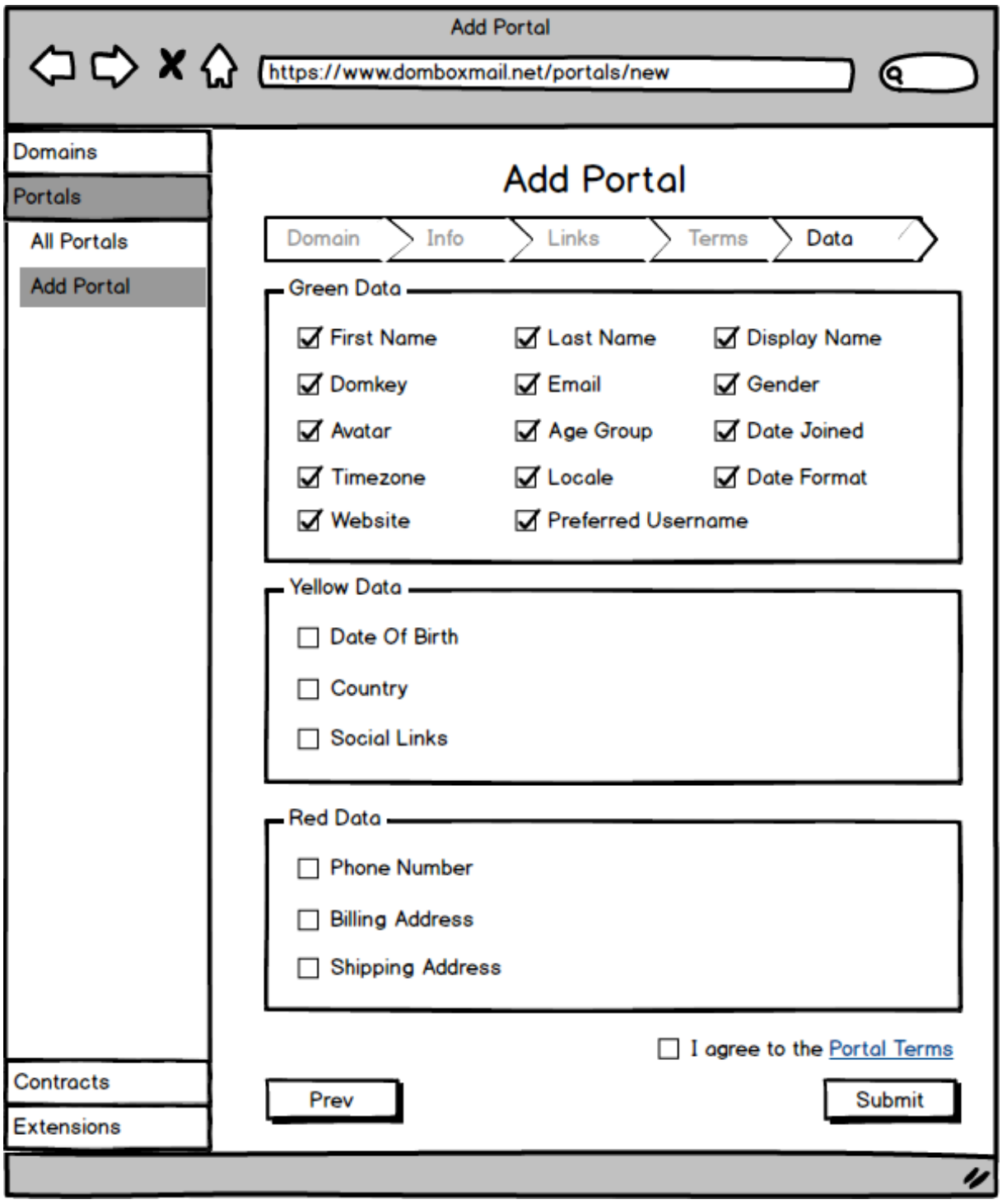


Figure 92: Business Side - Green Data

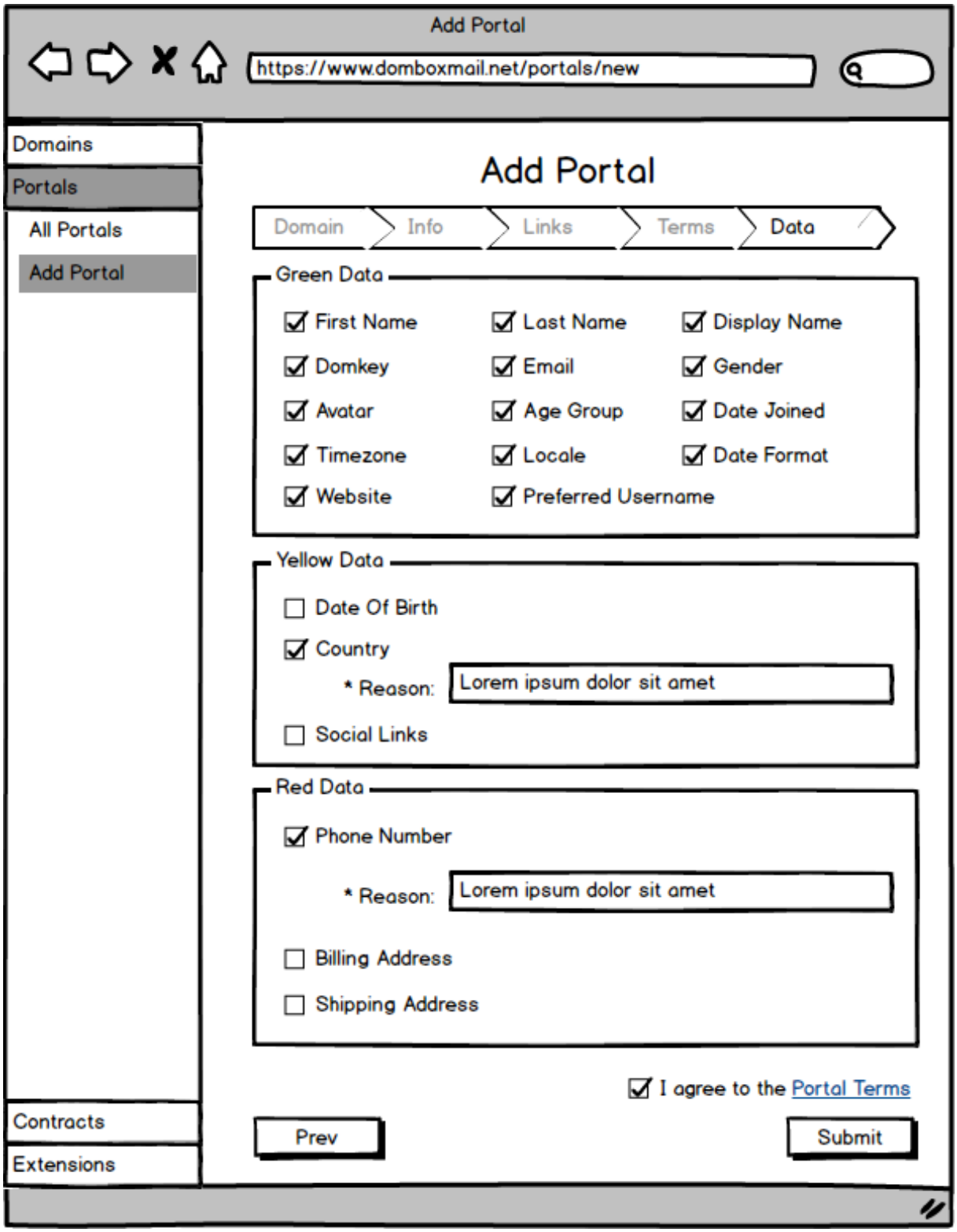


Figure 93: Business Side - Yellow and Red Data

Questions

Why should I use Teleport button instead of other Auth buttons like FB, Google etc?

Our "Teleport" button is created for a different purpose. You can put "Facebook Connect" and "Google Connect" buttons in the same bucket. But not the Teleport button. Our button brings some novelty.

All other buttons are like "Hello website owners, we have plenty of user data. Use our button and get access to any data you want"

But our Teleport button is like "Hello website owners, User privacy is Important. Use our button. Get limited data access that's essential for signup and login."

Besides, all other buttons have overcomplicated permissions.

Take Google as an example. Their button can give access to the whole account. A few years back, "Pokemon Go" app had the "Full account access". That means they have access to your Gmail, Contacts, Search History, Documents etc.. Why would a gaming app need all those permissions?

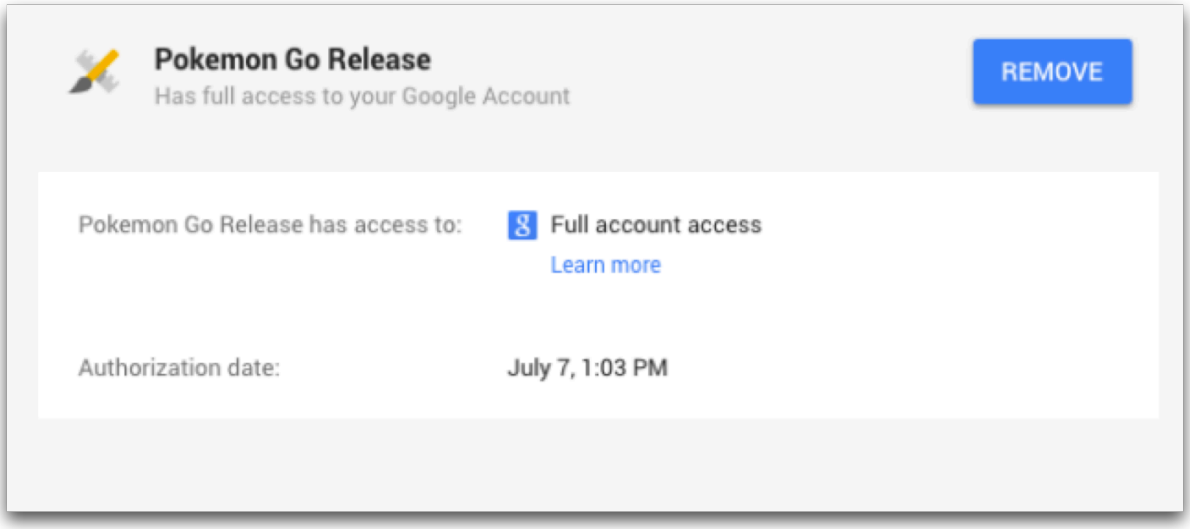


Figure 94: Pokeman Go Permission Issue

If you are reading this document up to this point, then you are not an average user. So you are one of the few people, capable of going through the app permissions before allowing the access. But an average user who is going to play the game don't have much patience in checking the App permissions.

As for Facebook, their "Cambridge Analytica" situation says everything.

"Teleport" button doesn't have these overcomplicated permissions.

These are the Unique Selling Points of Teleport.

1. Spamless
2. Better Privacy
3. Transparency
4. Simplicity

Spamless:

Teleport button creates an Isolated Mailbox and only 5 layer passed mails will be accepted.

Better Privacy:

Our Teleport button fixes one of the major privacy issue created by Gravatar. [Refer chapter 19 for more info]

Transparency:

You can clearly see what data you gave access to the website from your Combox page.

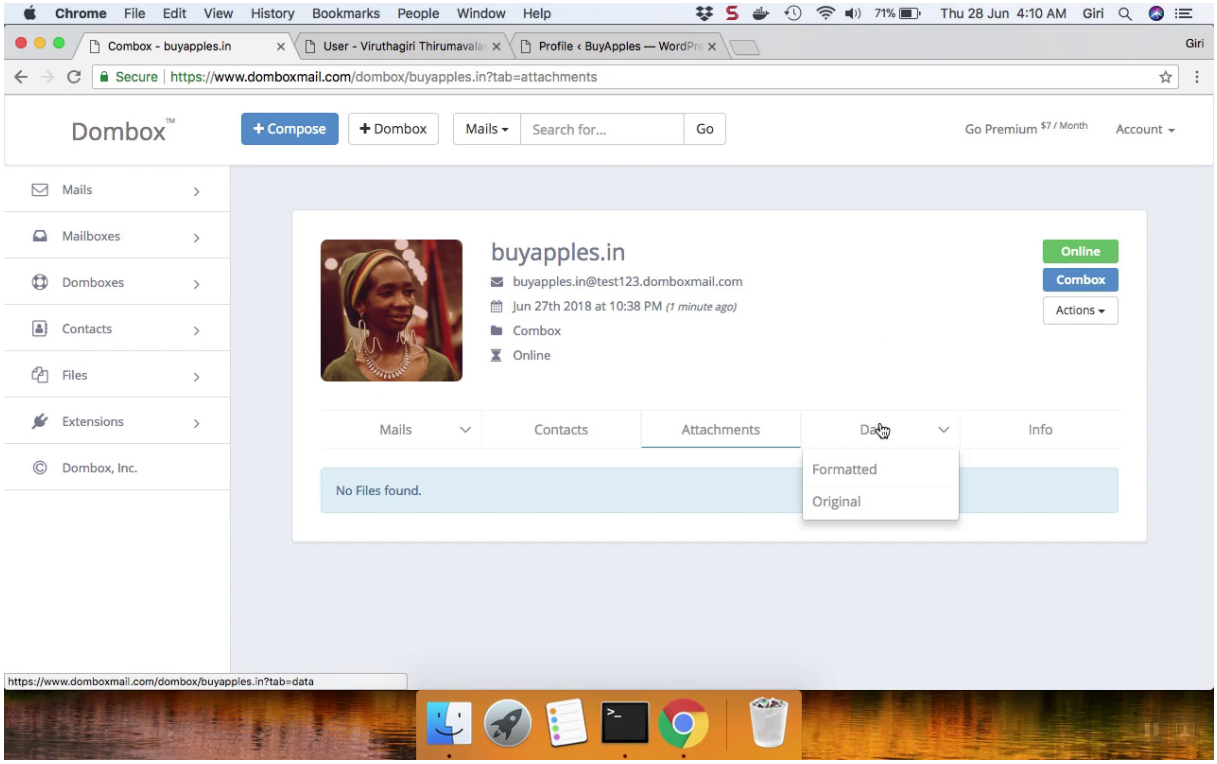


Figure 95: Data Tab

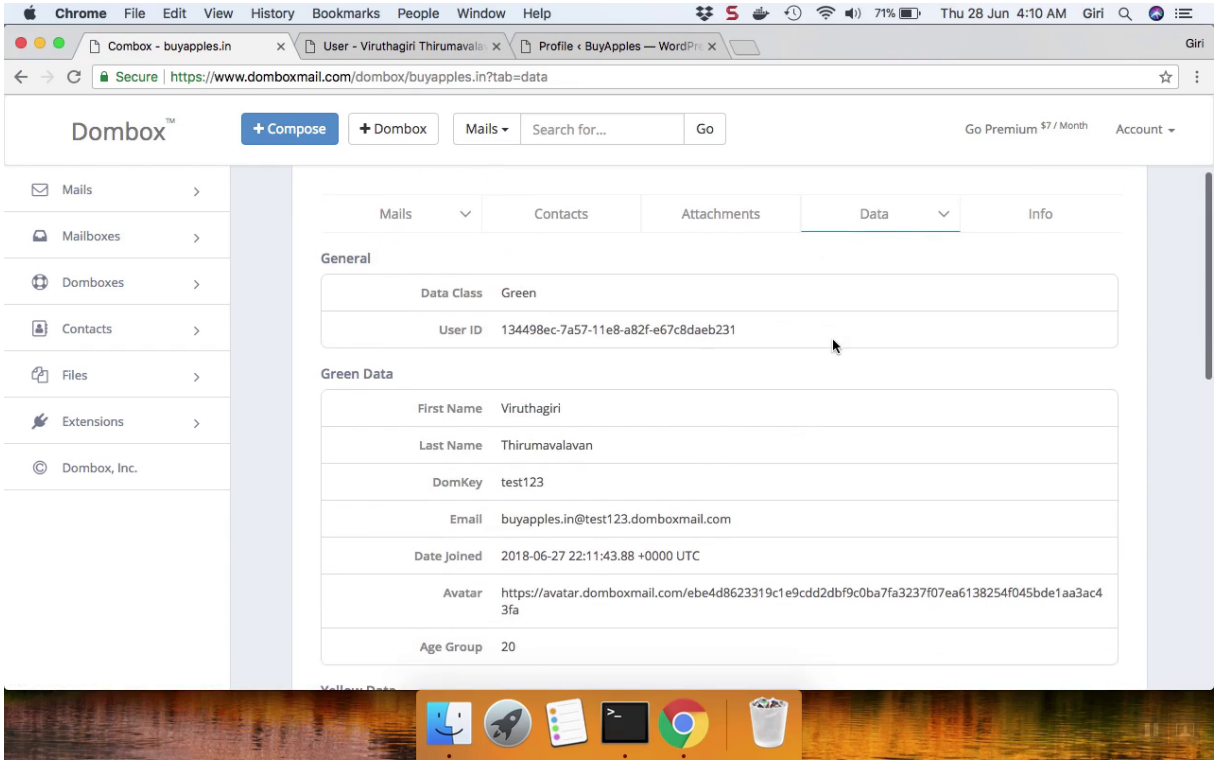


Figure 96: Data Formatted

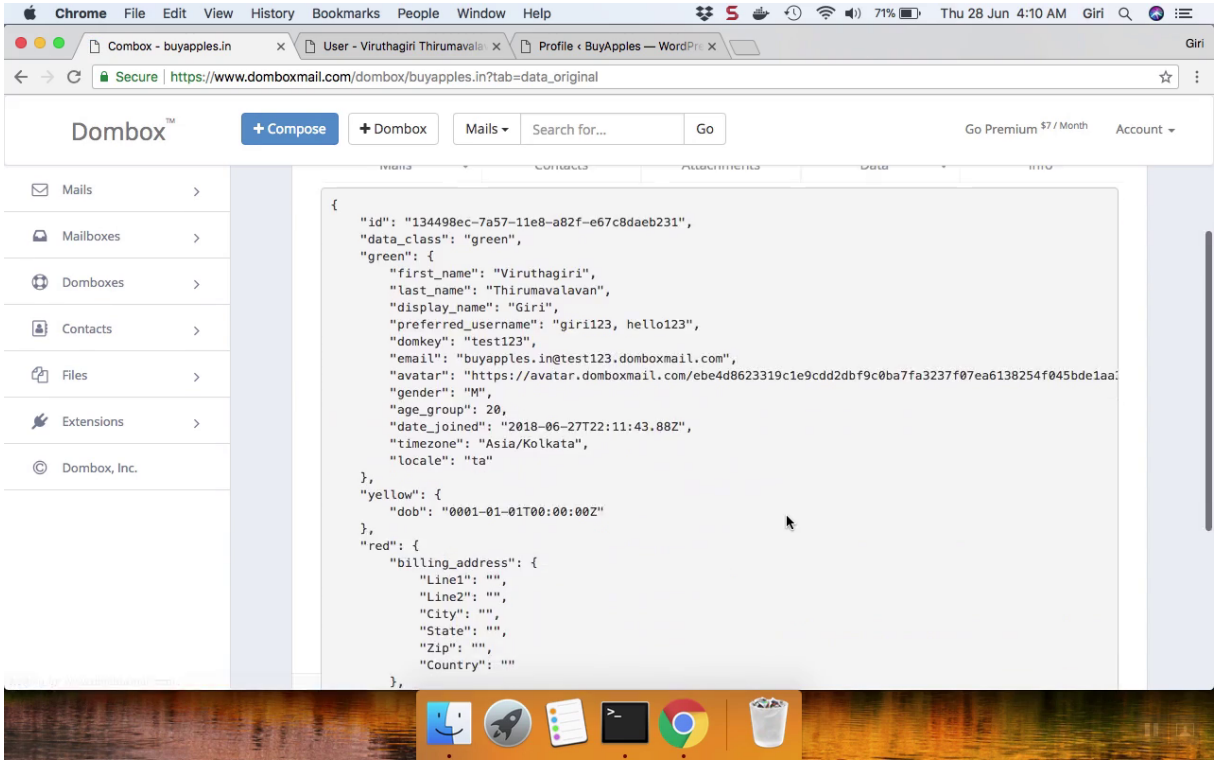


Figure 97: Data Original

Simplicity:

The purpose of Teleport button is Signup and Login. Nothing more. No other data access other than the fields you see in the traditional signup, login and edit profile forms.

Teleport button is designed to attract “Minimal Attention” from the user.

Data	Attention Level
Green Data	Looks Good
Yellow Data	Pay Attention
Red Data	Pay Strict Attention

Our “Teleport” consent screen interface is designed based on the Data Type.

If the Portal is “Red Portal”, then the interface will be in Red Colour. If it is a “Green Portal”, then the portal will be in “Green Colour”. So our “Teleport” button offers clarity.

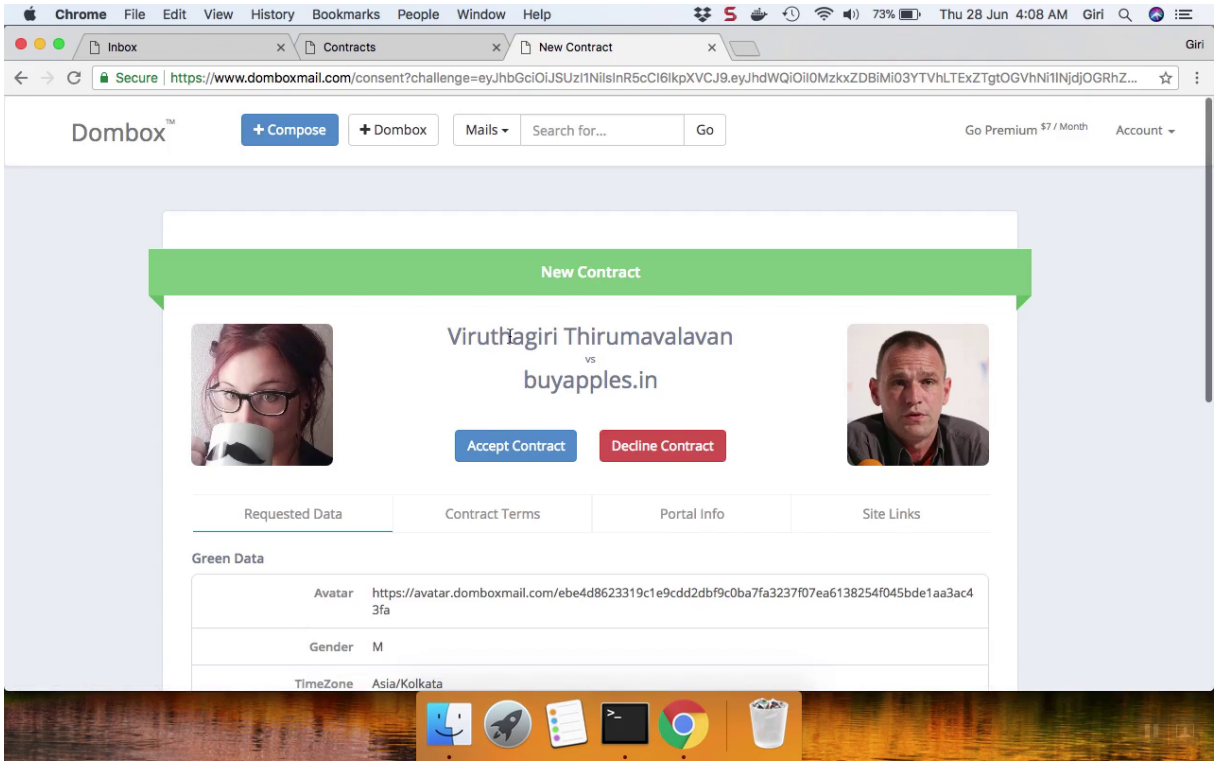


Figure 98: Green Portal Interface

Does that mean, developers cannot access any other data via API?

No.. We may allow developers to access other user data in the future. However, we will definitely brand the API differently.

In other words, If you see the term “Portal” and “Teleport”, then only those limited Green, Yellow and Red data fields can be accessed. Nothing more.

Because 99% of the time, when people click the “Signup with Google” or “Signup with

Facebook" kind of button, they are there to SIGNUP. Not to give access to their entire data.

Also, note that we are not a social networking website and we have no plans to become one. So there is no need for a website to put a message like "We don't share anything without your permission". So our button is "Less Scary".

Since the "Teleport" button only offers access to rarely changing data, there is no need for a "Revoke Access" button.

I'm a website owner, What makes you think I would become your Portal Partner?

You would become our Portal Partner only if your website supports our "Teleport" button.

Teleport button is not a mandatory thing. So you should support our Teleport button only if you really wants that. Not because we are saying so.

Our system would work even if none of those 332 million domains never support our Teleport button.

However, we recommend you to configure Teleport button for the following reasons.

1. Teleport button helps you with the "Unstable Users" problem.
2. Teleport button helps you with the "Data Breach" problem.
3. Teleport button says that you *care* about your users since you are making the signup process easier.
4. Teleport button says that you are taking your users privacy very seriously and you don't make your living by selling your users data.

When is the right time to become Portal Partner?

You can become our Portal Partner anytime. However, if you want to take control of all of your users from Day 1, then we suggest you to become our Portal Partner in one of the following situations.

1. Before we launch our product
2. Before you launch your product

domboxmail.com targets consumers and domboxmail.net targets businesses. We will be launching domboxmail.net at least a week before launching domboxmail.com. So you can create “Portal” apps for your website.

That way you can take control of your users from Day 1.

If you miss that and configure Teleport button later (e.g. after a year), then you may have to let some dombox users (i.e. The ones who created dombox manually) use your service without any contract. You can force them to sign the contract when they try to login next time. But that can also cause negative effects. Some users would delete the box and move on.

Keep in mind, your mail needs to pass all 5 layers to become our Portal Partner. So make sure to configure those layers in the meantime.

I’m a website owner, But I have no idea how to configure those five layers?

If you have no idea, then we presume you are a non-techie. Hopefully, you are on a “Managed Web Hosting” plan. Just go to your web hosting support section and open a support ticket with a subject like “Help me to configure Dombox Layers”. They can probably assist you in this case.

As the name says, they are there to manage. So it’s their job to help you in cases like this. Also note, Except the “Alias Layer”, all other 4 layers can help fight spam in other mail services too. So you don’t have to wait till we release our product.

We have plans to invest money in creating “How To” videos for all those 5 layers. These videos gonna be DIY kind of videos. We also have plans to have Sandbox for each layer. So you can send mails and test it there.

I’m a website owner, How do I setup Teleport button?

If you are using a popular open source software like WordPress, then you can install the “Portal Client” in few clicks.

Also, we will be releasing “Portal Client” libraries for most popular programming languages with Documentation. So if you are a programmer, you can integrate that easily.

Chapter 12: Telescribe

Box Type: Hybrid (H)

Hybrid (H) box is the same as Combox (C) except it can be put offline and deleted.

Or you could say Hybrid (H) box is the same as Dombox (D) except it needs to pass all 5 layers.

Hybrid (H) box offers both Dombox (D) features as well as Combox (C) features.

So it's a love child of Dombox (D) and Combox (C)

Hybrid (H) box type can be helpful in three situations

Situation	Description
Telescribe	Our "One-Click" newsletter subscription service
Upgrade	Consumers can voluntarily upgrade from "Dombox" to "Hybrid" if they are absolutely sure that the website "Pass" all 5 layers
Downgrade	When a contract gets terminated, the box will be downgraded from "Combox" to "Hybrid".

Dombox vs Hybrid vs Combox

	Make Offline?	Delete?	All 5 layers must be passed?
Dombox (D)	Yes	Yes	No
Combox (C)	No	No	Yes
Hybrid (H)	Yes	Yes	Yes

Telescribe

Have you ever signed up for a newsletter in 3rd party websites? It usually looks something like this.

A name field. An email field. And a Submit button. Title of this form usually be “Subscribe to our Newsletter”

When you fill the form and submit, the process is called Single Opt-In.

Now some newsletter services require a confirmation. So you will get a confirmation email.

If you confirm by clicking the link, then you become a subscriber. This confirm process is called Double Opt-In.

Think about it. What’s stopping someone from submitting your email address in a newsletter subscription form. In order to prevent email misuse, a website requires the Double Opt-In process. Otherwise, the website may be spamming people.

To make this process easier, We are introducing a button called “Telescribe”.

Well… Think of it like a Facebook Like or Twitter Follow button you see on websites, but for email newsletter subscription.

So its a “One-Click Subscribe” button

When you click the “Telescribe” button, a Hybrid (H) box will be created for the domain

Telescribe button is not an alternative to 3rd party newsletter services like MailChimp. You still need to depend on 3rd party newsletter services. Telescribe button only makes the subscription process easier.

Keep in mind, if a box already exists for that domain, then only the subscription status will be changed.

Telescribe button can be displayed by any website by adding our telescribe.js file. In fact, a website owner can display other website’s “Telescribe” button too

When a user clicks the “Telescribe” button, it creates only a “Hybrid (H)” box

So anyone can display the “Telescribe” button. But only the “Dombox Domain” and its SAD Domains can send the mail to the box (Since its a Hybrid box, it requires a pass for all 5 checks. Also it can be deleted and put offline by the user)

A consumer can Unsubscribe via the same “Telescribe” button.

If the consumer uses the same Telescribe button to unsubscribe, then the box will get deleted if it meets the following conditions.

1. The box is a Hybrid box
2. The box was created via Telescribe button
3. The box is a Virgin box. {Meaning… No emails ever received to that box}

If those conditions are not met, then only the box subscription status will be changed to “Unsubscribed”.

See the illustration in the next few images

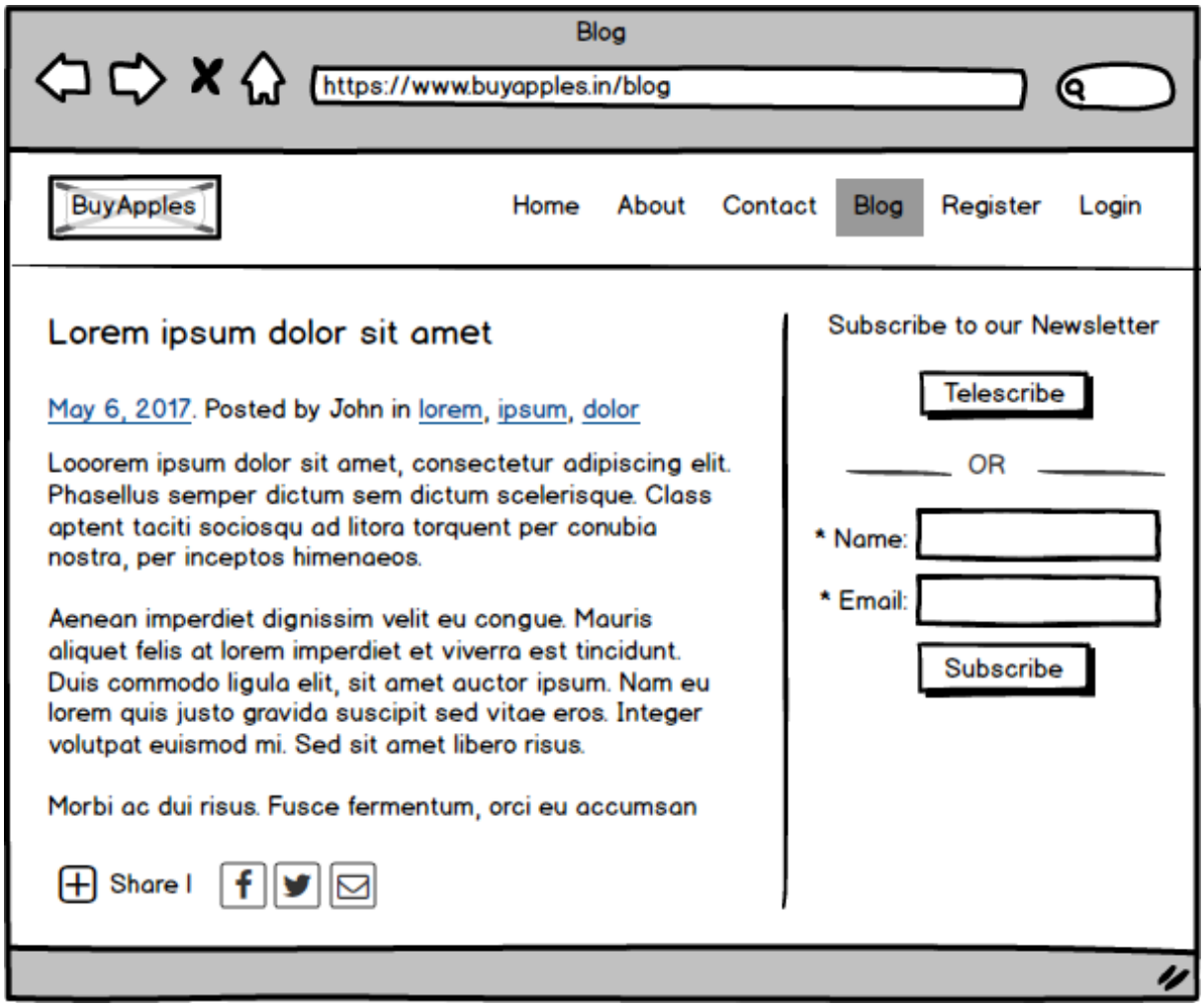


Figure 99: Telescribe button added via telescribe.js

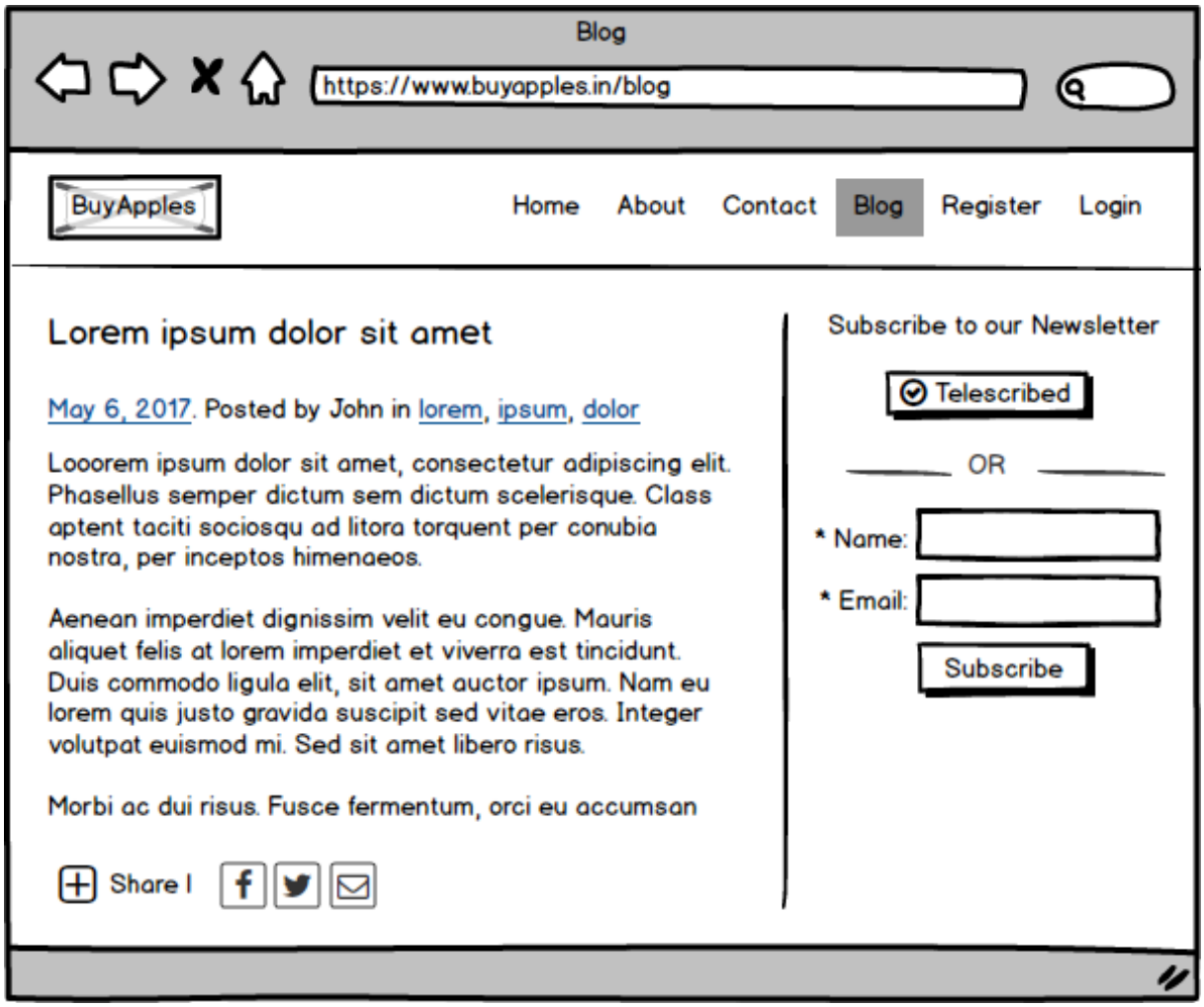


Figure 100: Button view when Subscribed

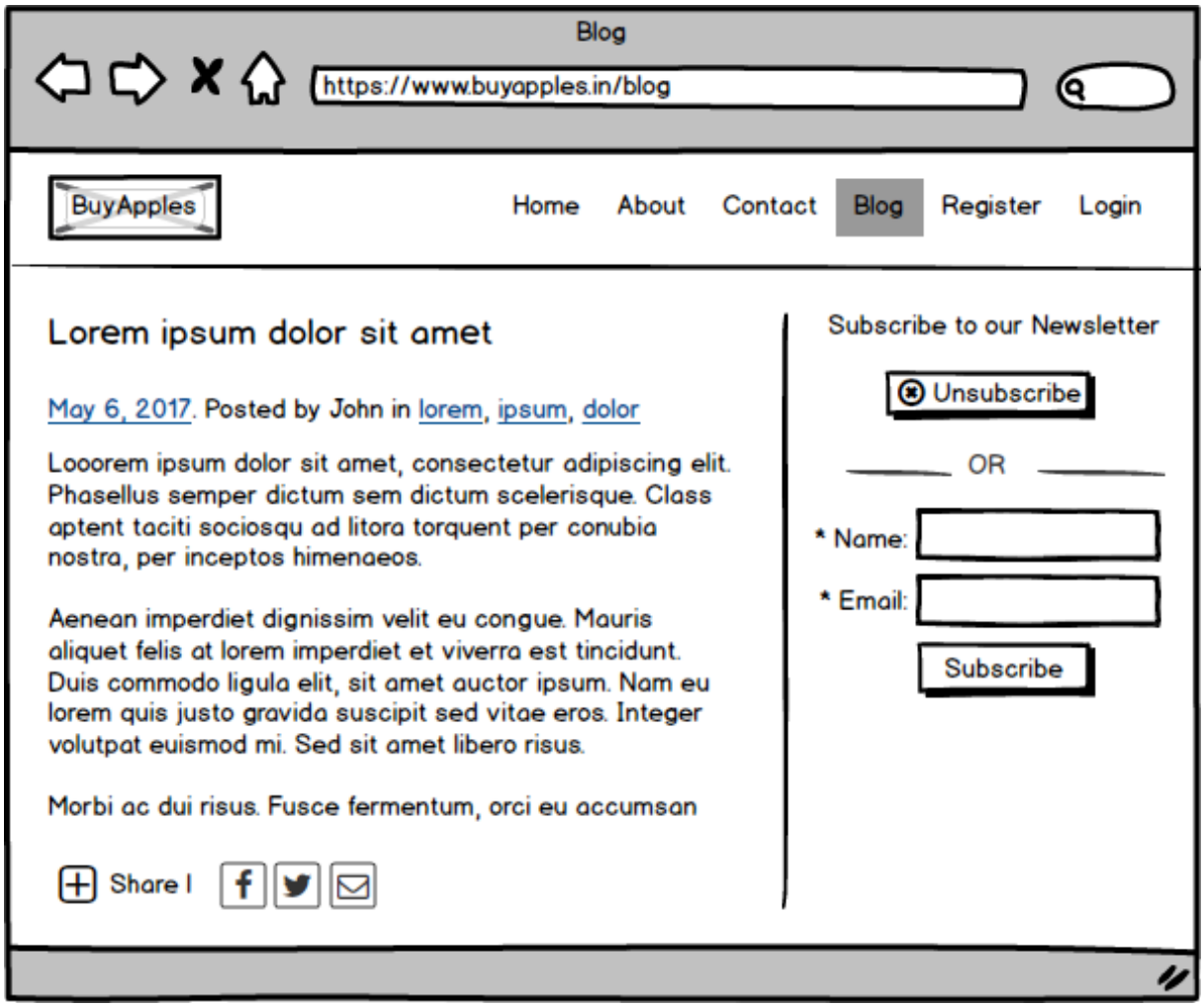


Figure 101: Button view when Hovered

Subscribers

Telescribe button will be used for Subscribe / Unsubscribe

However, Consumers can also Subscribe / Unsubscribe from the box itself

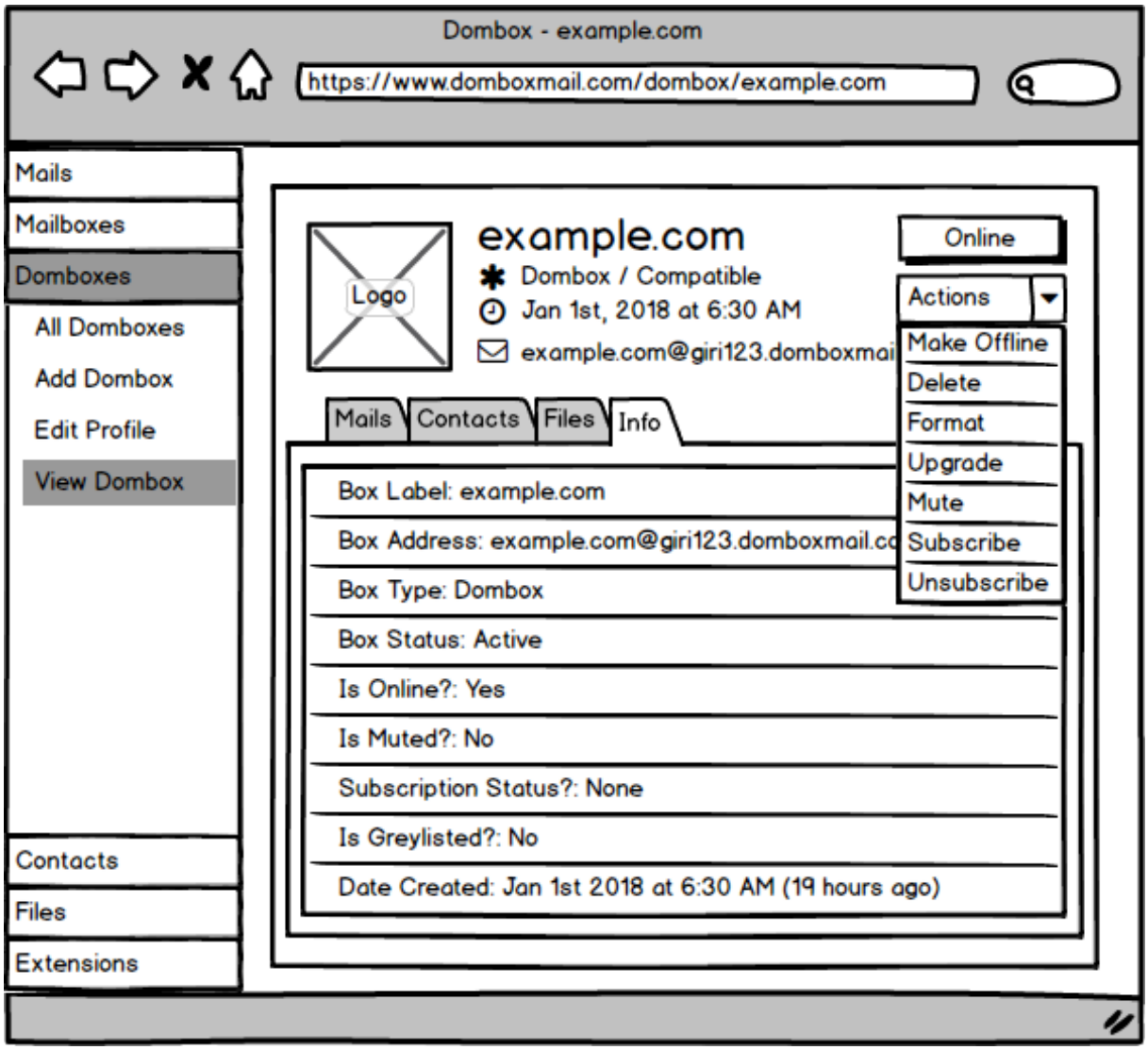


Figure 102: Subscribe / Unsubscribe

As for the domain owners, Domain verification is necessary to access the “Subscribers” data, but “Good Standing” is not a requirement unless your domain is a “Portal Partner”

Domain owners can access the “Subscribers” data via API in the future.

To view subscribers, the website owner needs to activate the “Subscribers” extension.

We will also have an Extension called “Subscriptions” for consumers. This will list all their

subscriptions

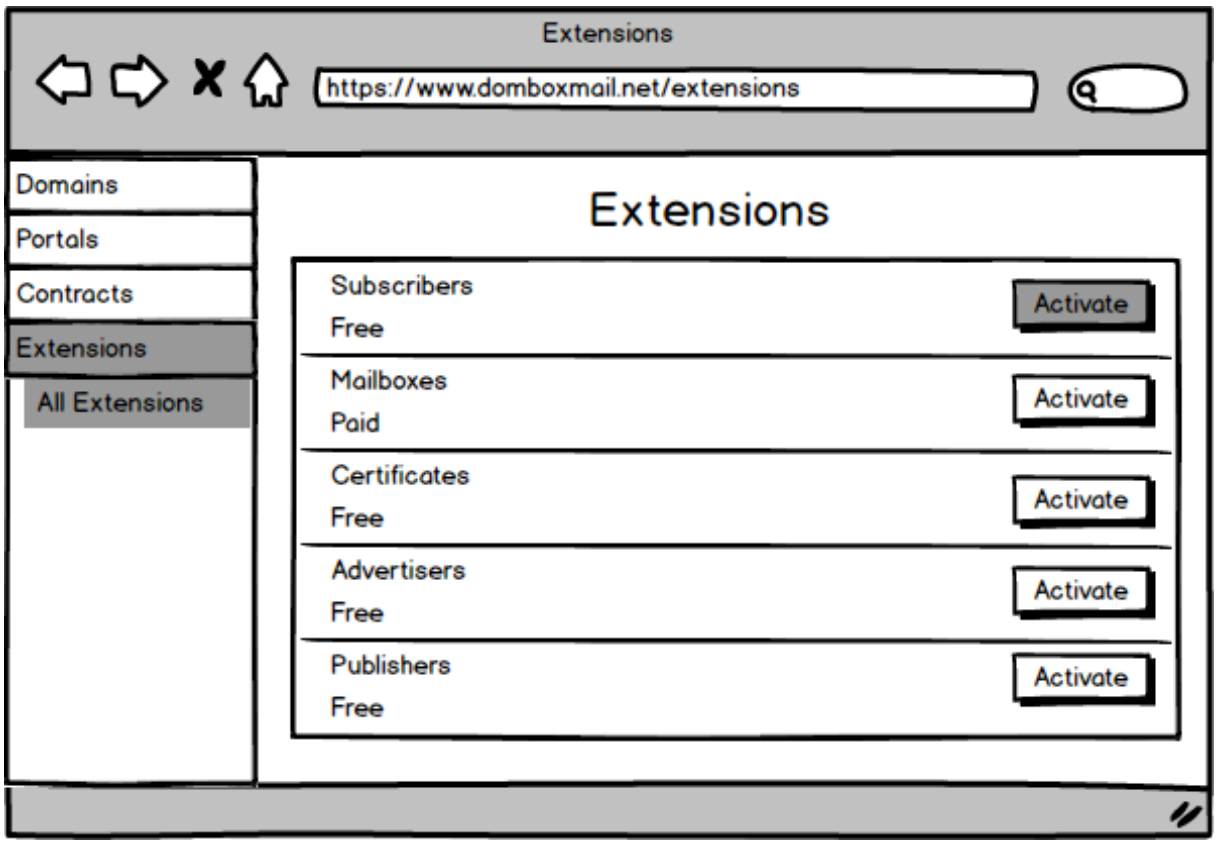


Figure 103: Subscribers Extension Activation

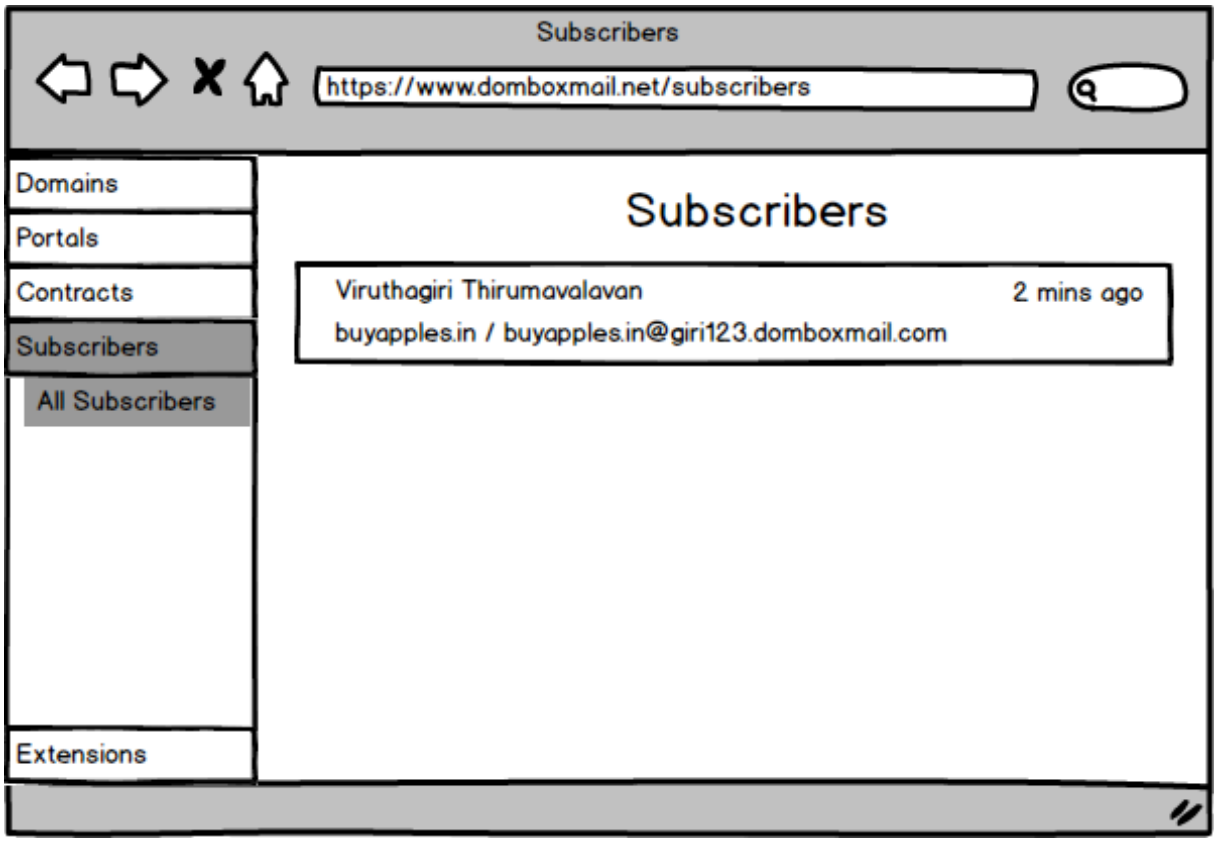


Figure 104: Subscribers

Managers

We will be providing API for 3rd party newsletter services with "Webhooks" support. We call these 3rd party newsletter services as "Managers".

Just like a website become our "Portal Partner", third party newsletter services can become our "Managing Partner" [Note: This term has nothing to do with Dombox, Inc. company Management]

You will be seeing a button like "Manage My Domain" or "Manage My Subscribers". [We have not decided the proper button name. You are welcome to suggest one]

In the "Teleport" button, the "consumer" is giving permission to "Dombox, Inc." to let the

"Business Owner" access their personal data

In "Manage My Domain" button, the "Business Owner" is giving permission to "Dombox, Inc." to let the "Manager" access their subscribers data

Keep in mind, "Managers" will have access to only limited data. Full Name, Email, Subscription Status and Date Subscribed [Maybe we should allow all "Green" Data since its insensitive?]

Chapter 13: Contacts

By default, all contacts in your "Address Book" will be considered as "Neutral" contacts

But you can "Whitelist" a contact if the contact is a very important contact. We will be less aggressive with that contact when passing their mails via Spam / Anomalies Filter.

You can also "Blacklist" a contact. We will reject emails from that contact immediately.

If a contact is whitelisted, you will see a "Green Checkmark" right next to the contact name.

If a contact is blacklisted, you will see a "Red X mark" right next to the contact name.

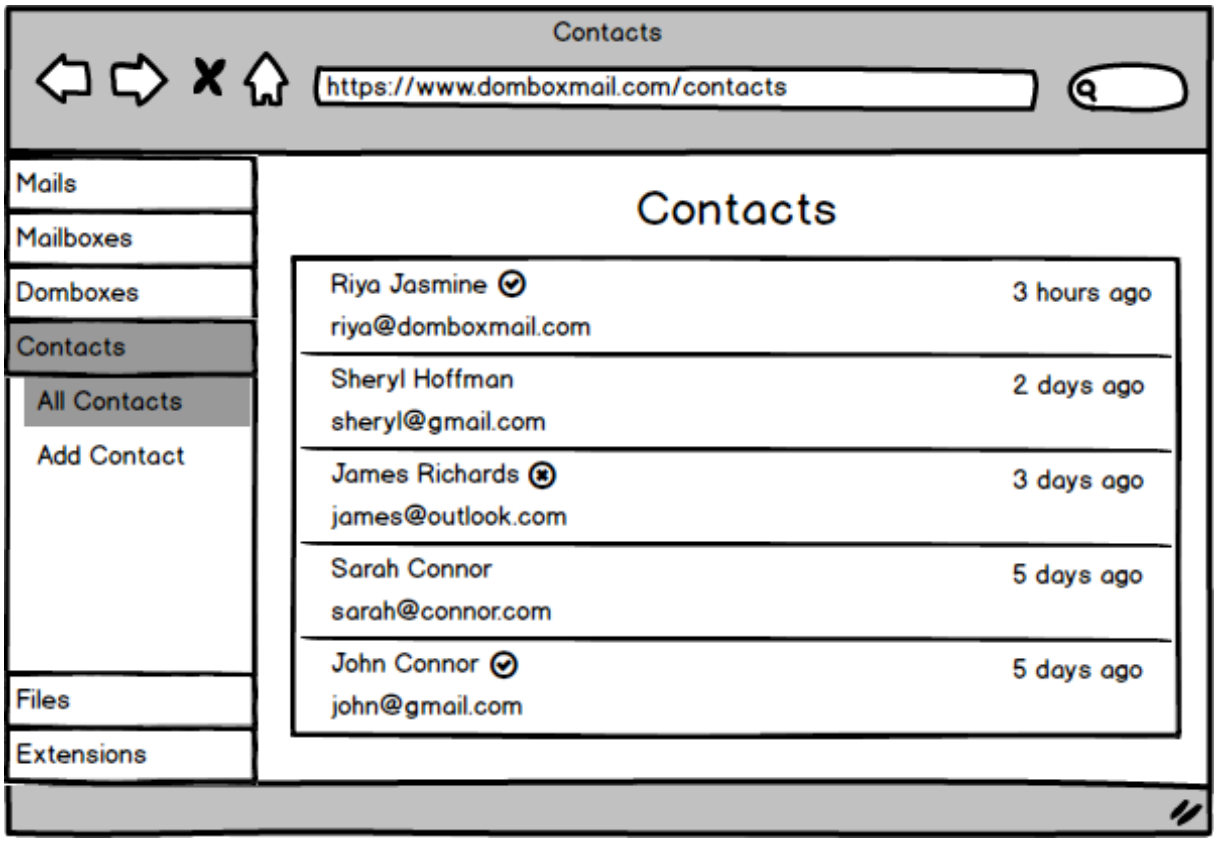


Figure 105: Contacts - List View

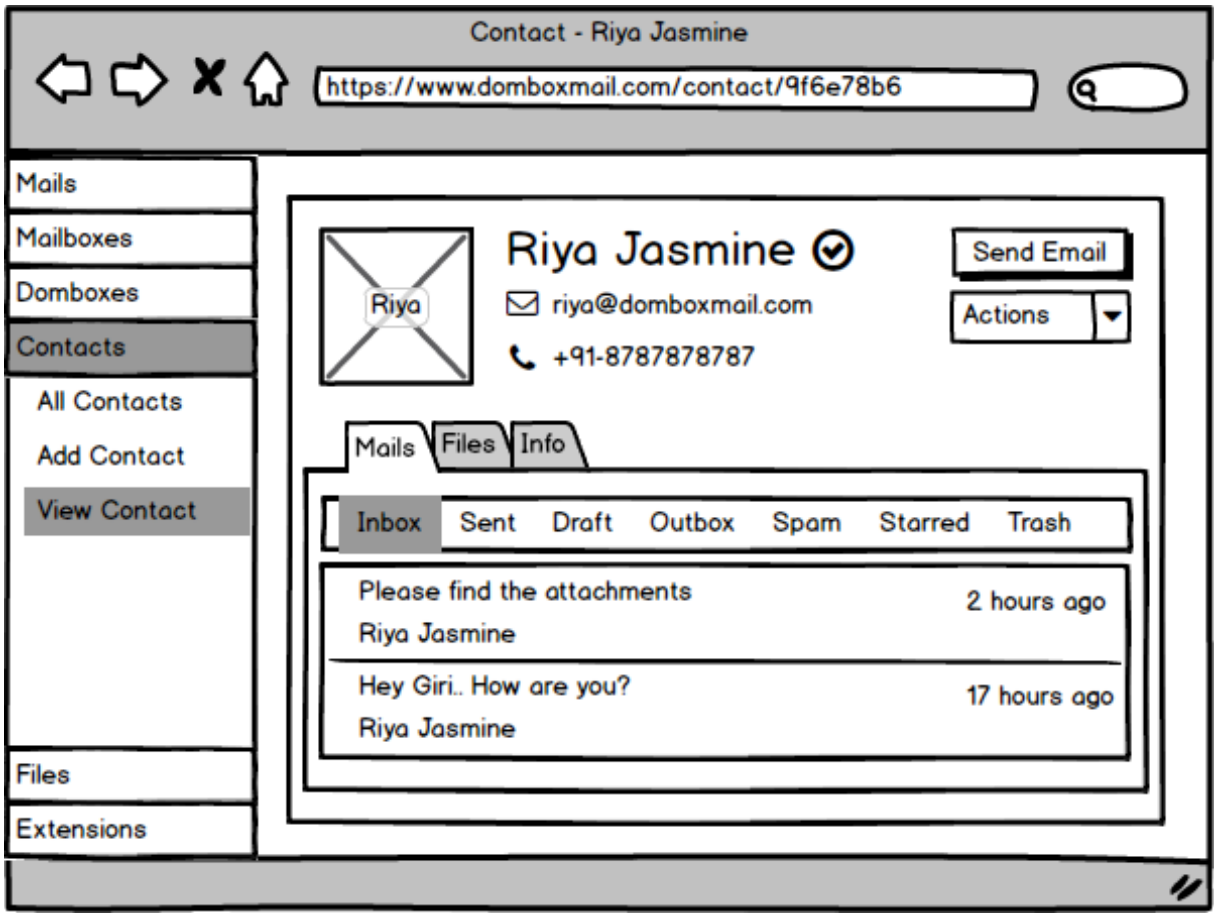


Figure 106: Contacts - Mails View

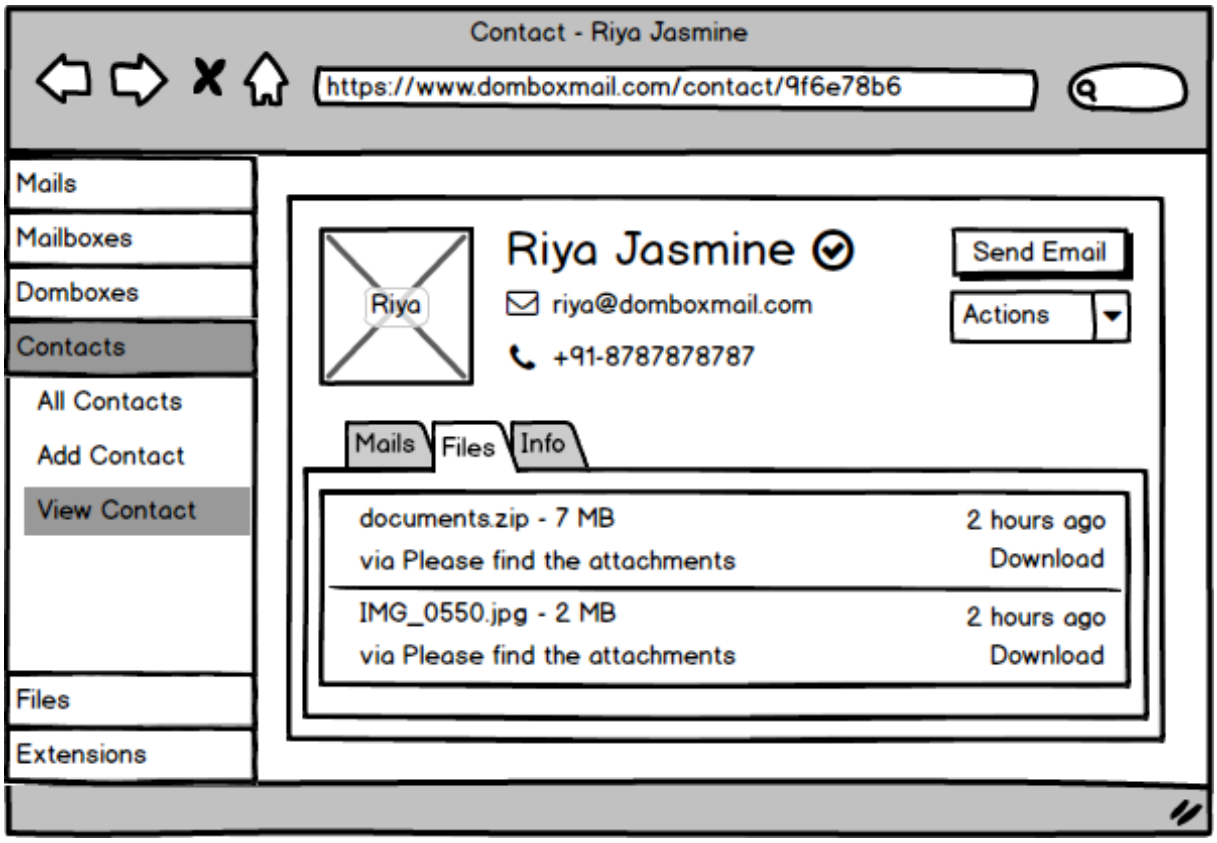


Figure 107: Contacts - Files View

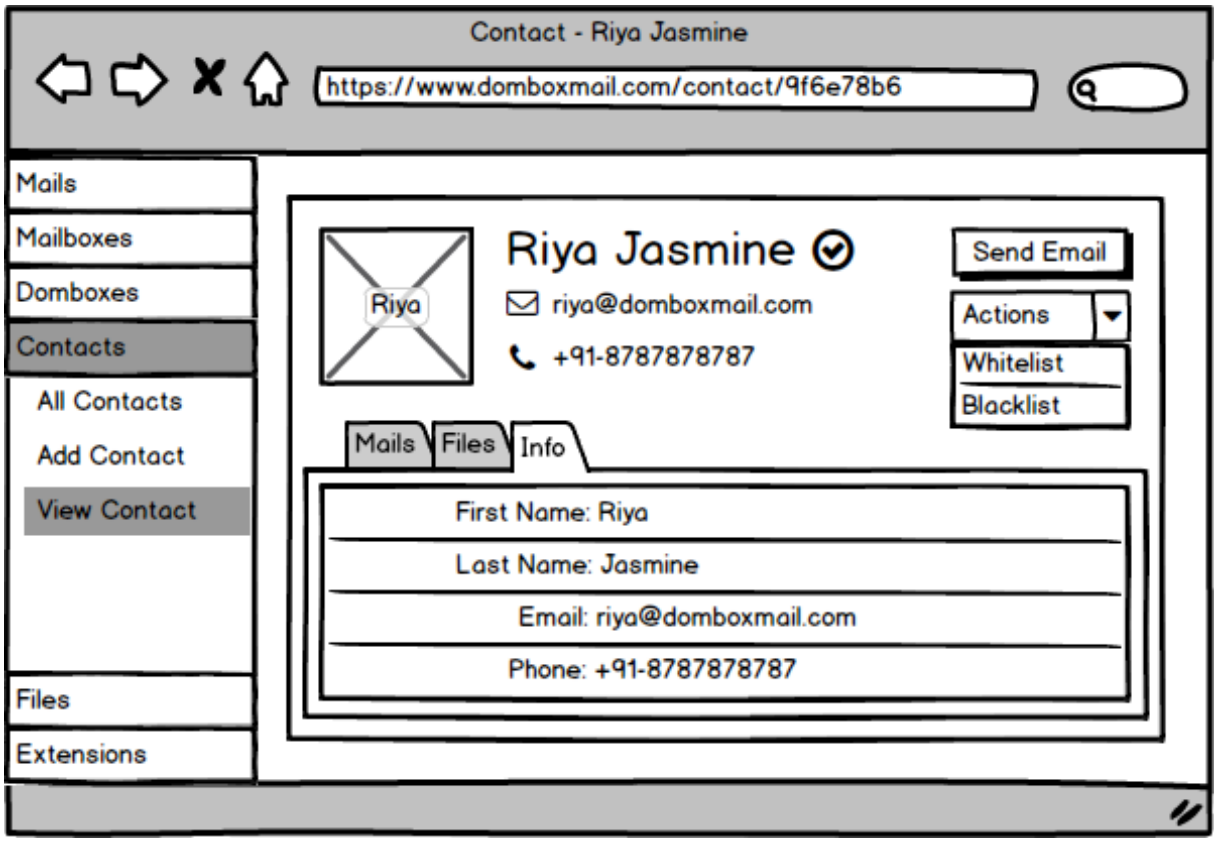


Figure 108: Contacts - Info View

Chapter 14: Files

The “Files” section, contains all the files. Received, Sent, Uploaded, Shared etc.

If you see a “Green Checkmark” right next to the file name, then its a clean file (i.e. Contains no virus).

If you see a “Red X mark” right next to the file name, then it contains the virus. So proceed with caution.

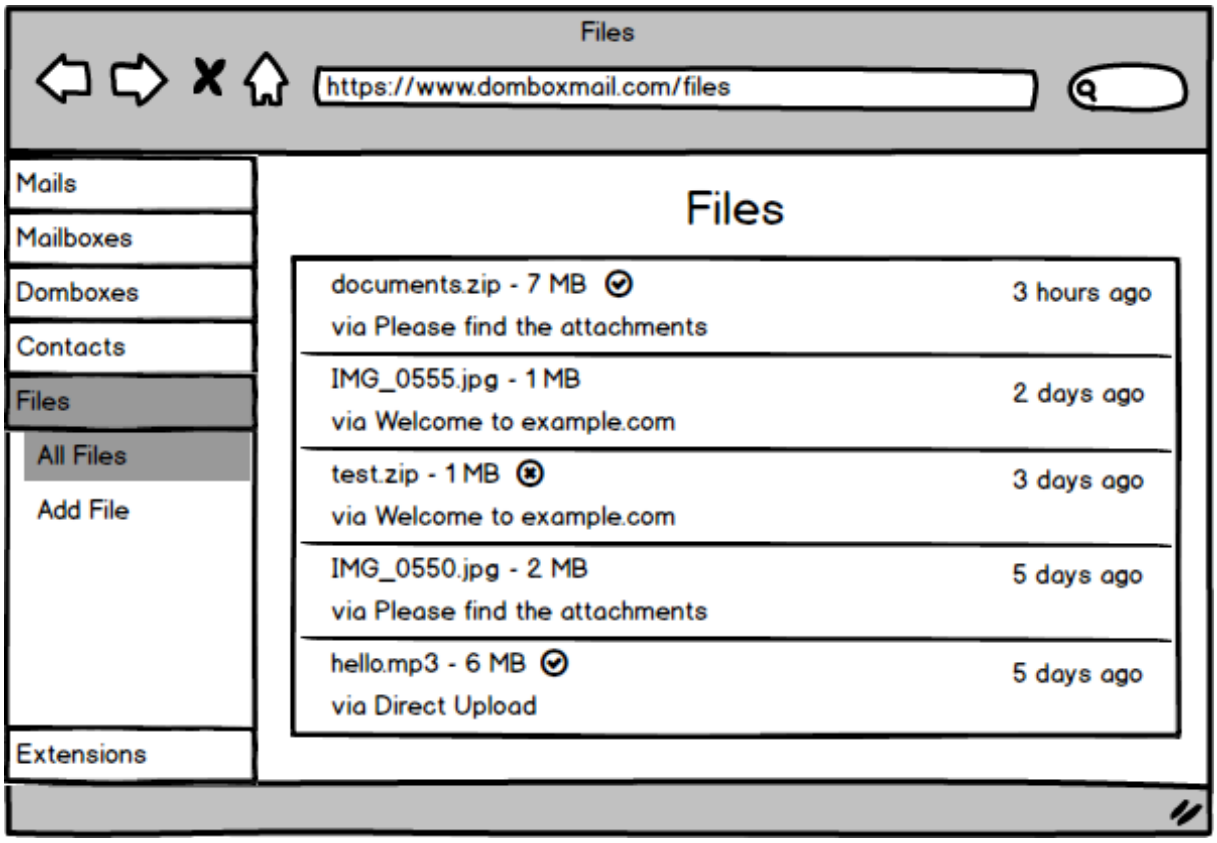


Figure 109: Files - List View

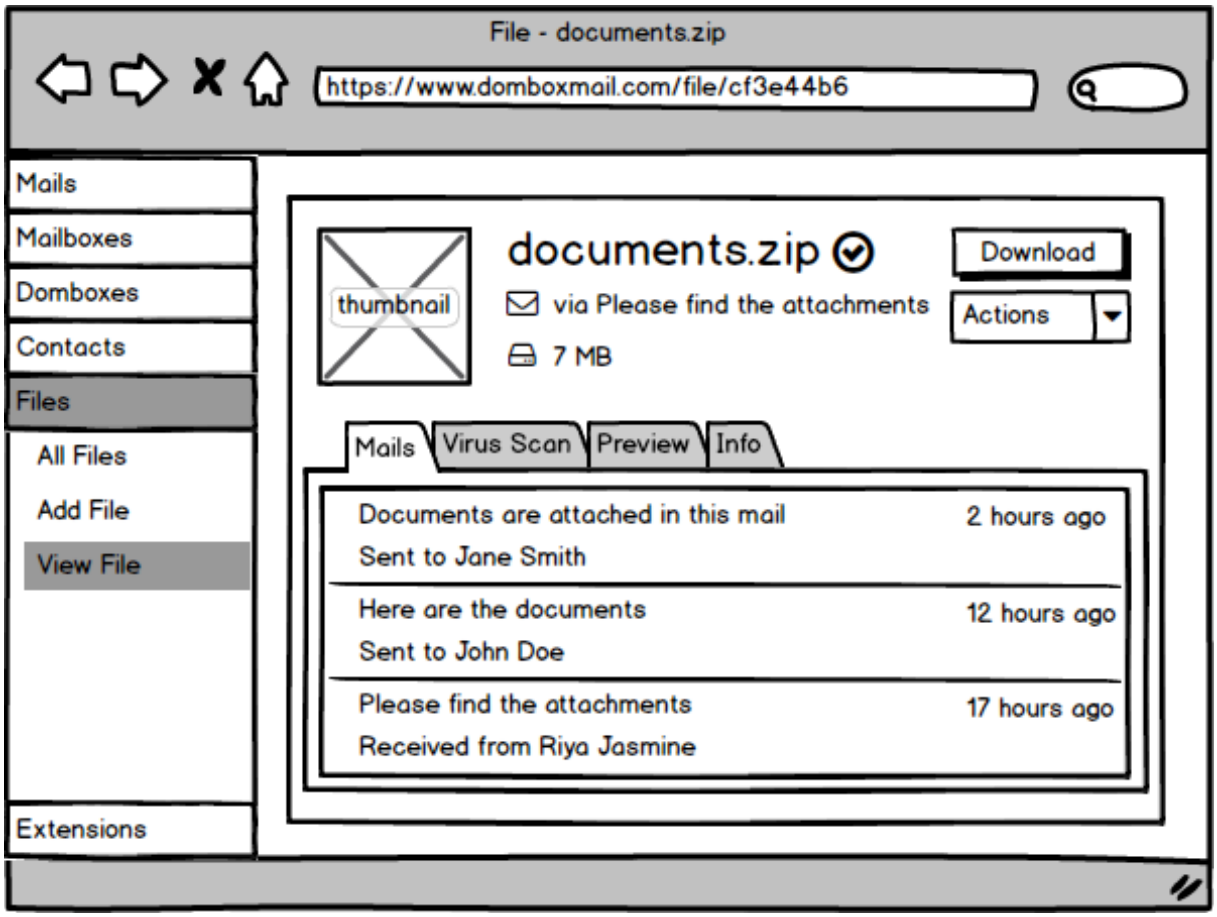


Figure 110: Files - Mails View

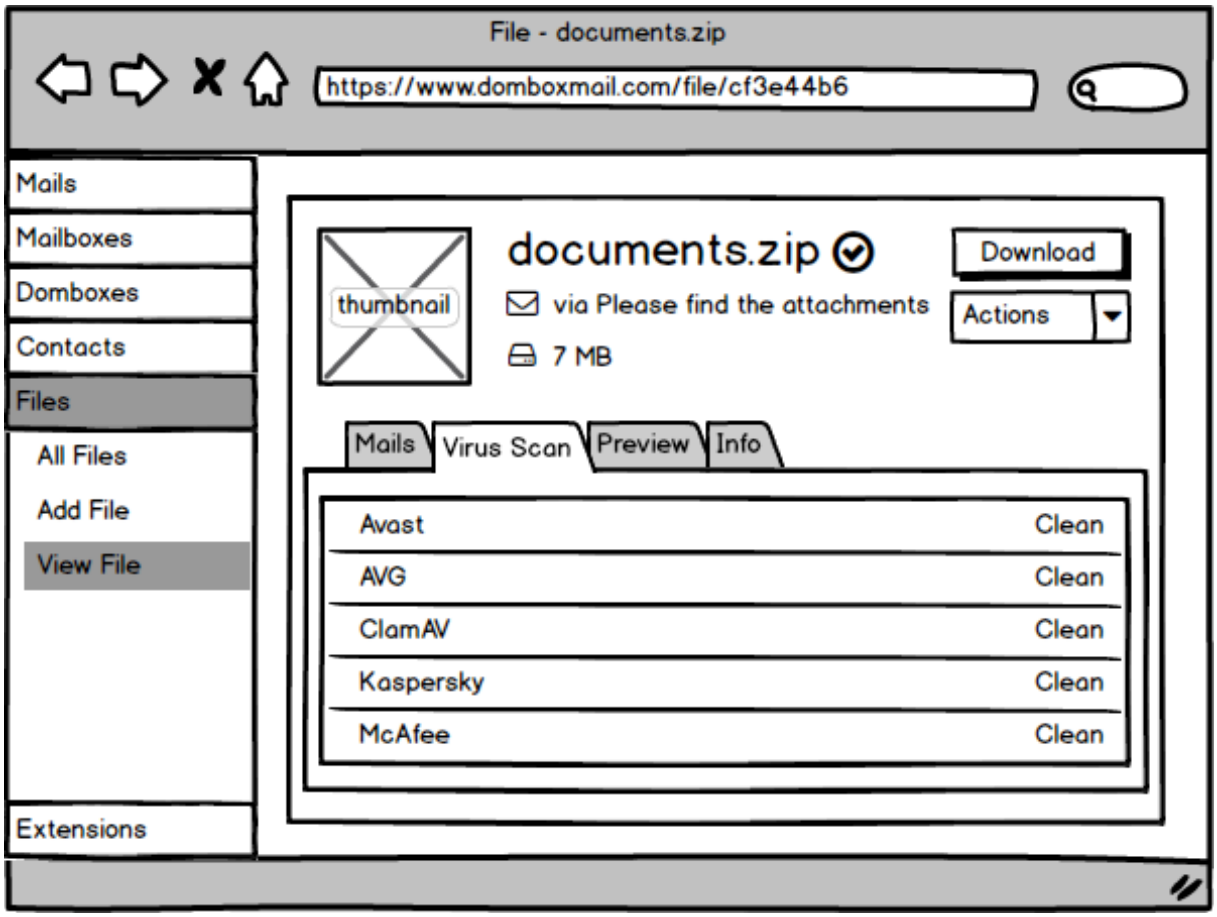


Figure 111: Files - Virus Scan View

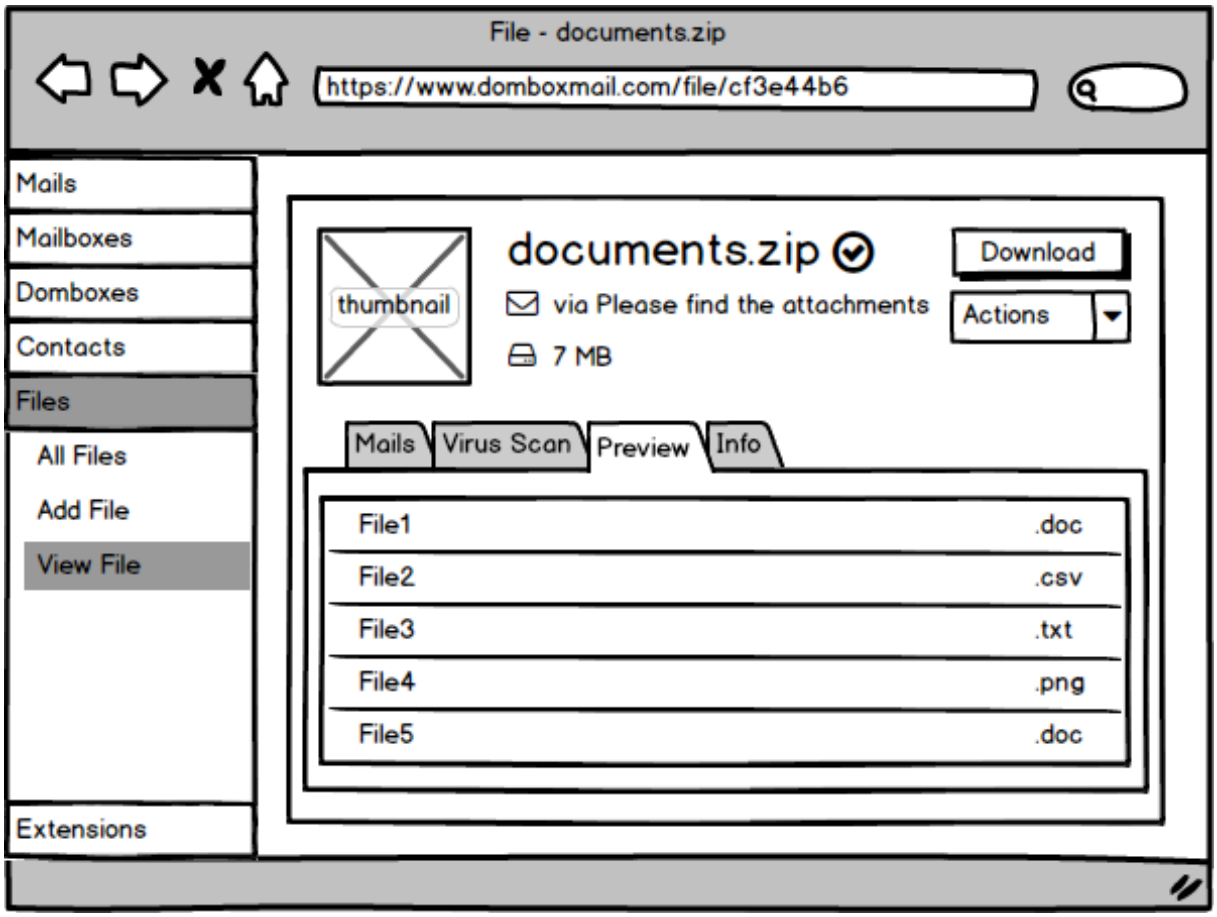


Figure 112: Files - Preview

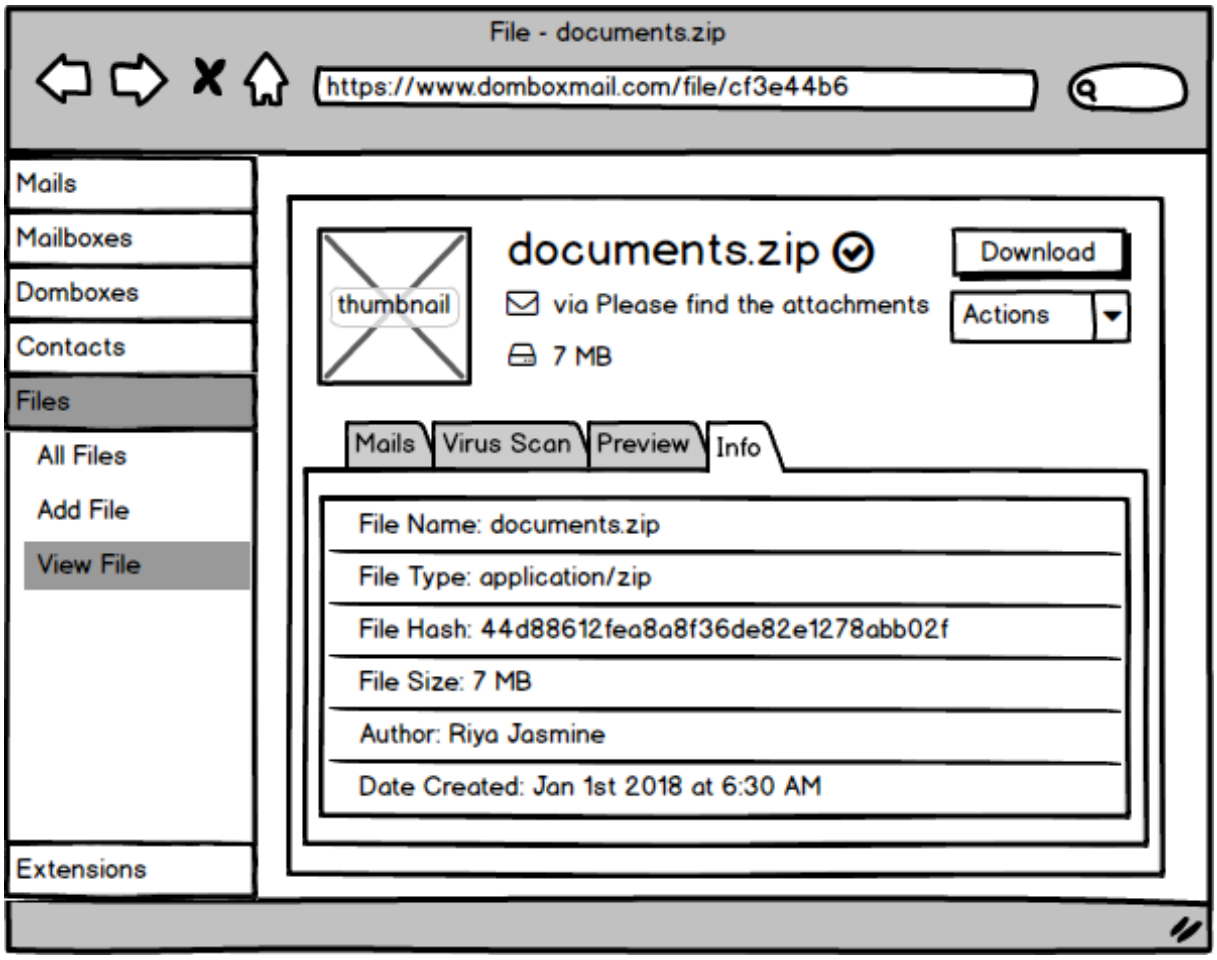


Figure 113: Files - Info View

Chapter 15: Restriction

The Problem

"Domboxes" definitely gonna protect you from spammers because each dombox can receive emails only from the "Dombox Domain" and its "SAD Domains".

But what about "Mailboxes"? They can receive emails from anyone, right?

For instance, what happens when your Primary (P) mail address somehow end up in a

spammer's hand? There are ways a spammer can acquire your primary email address.

e.g. These days every app ask you to invite your friends. We have friends who sell us out by giving full access to their "Google Contacts" and "Facebook Contacts" for some extra life in games. Most likely you have such friends too.

So a hacker can hack those app servers and get your contact from there. A hacker can also post the data dump in public forums.

The trick is not in preventing spammers from getting your primary email address. It's in making your primary email address useless in the spammer's hands. i.e. Spam should be prevented at the source, not the destination.

Figure 114: Restricted Area

So.. Who are these “authorized personnel”?

Well... That’s the Whitelisted and Neutral contacts found in your “Address Book”.

Restriction Phase actually contains two modes

1. Restricted Mode
2. Greylisted Mode

Restricted Mode

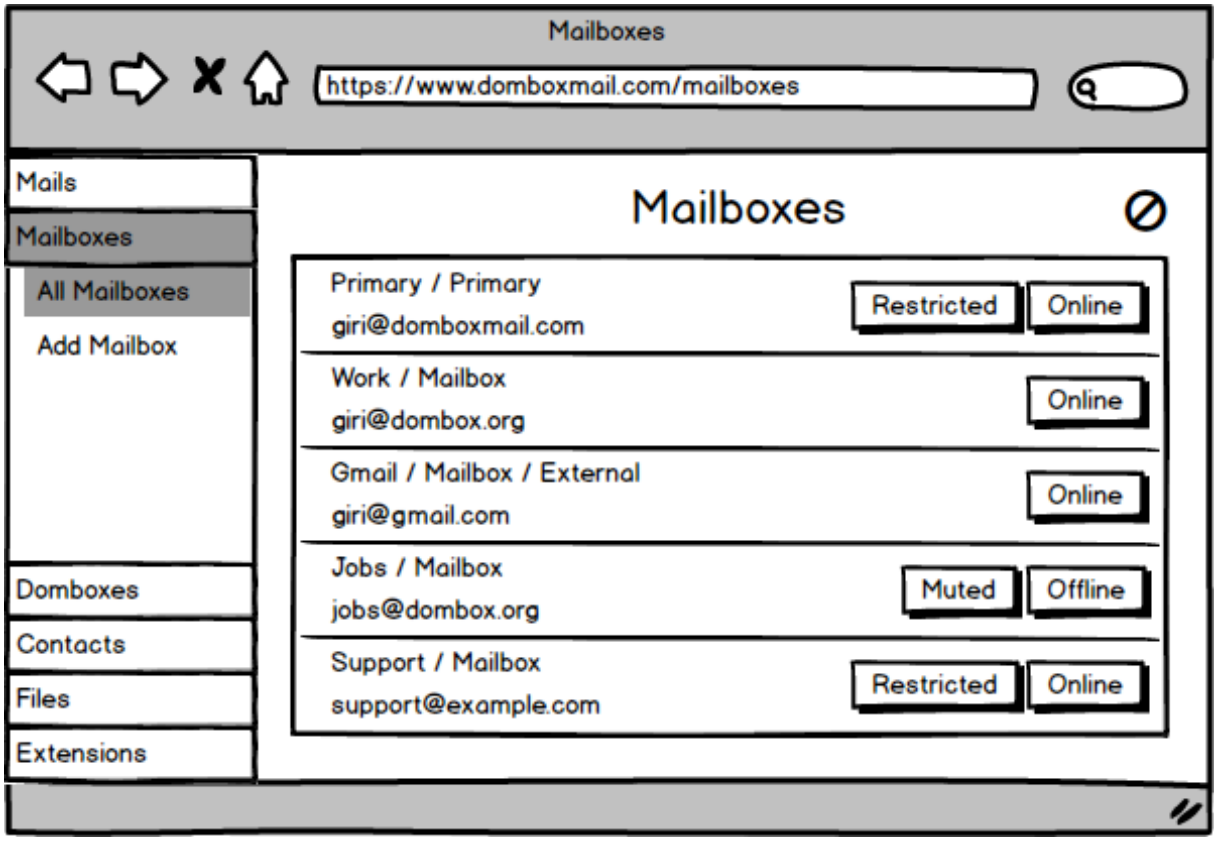


Figure 115: Restricted Mode - List View

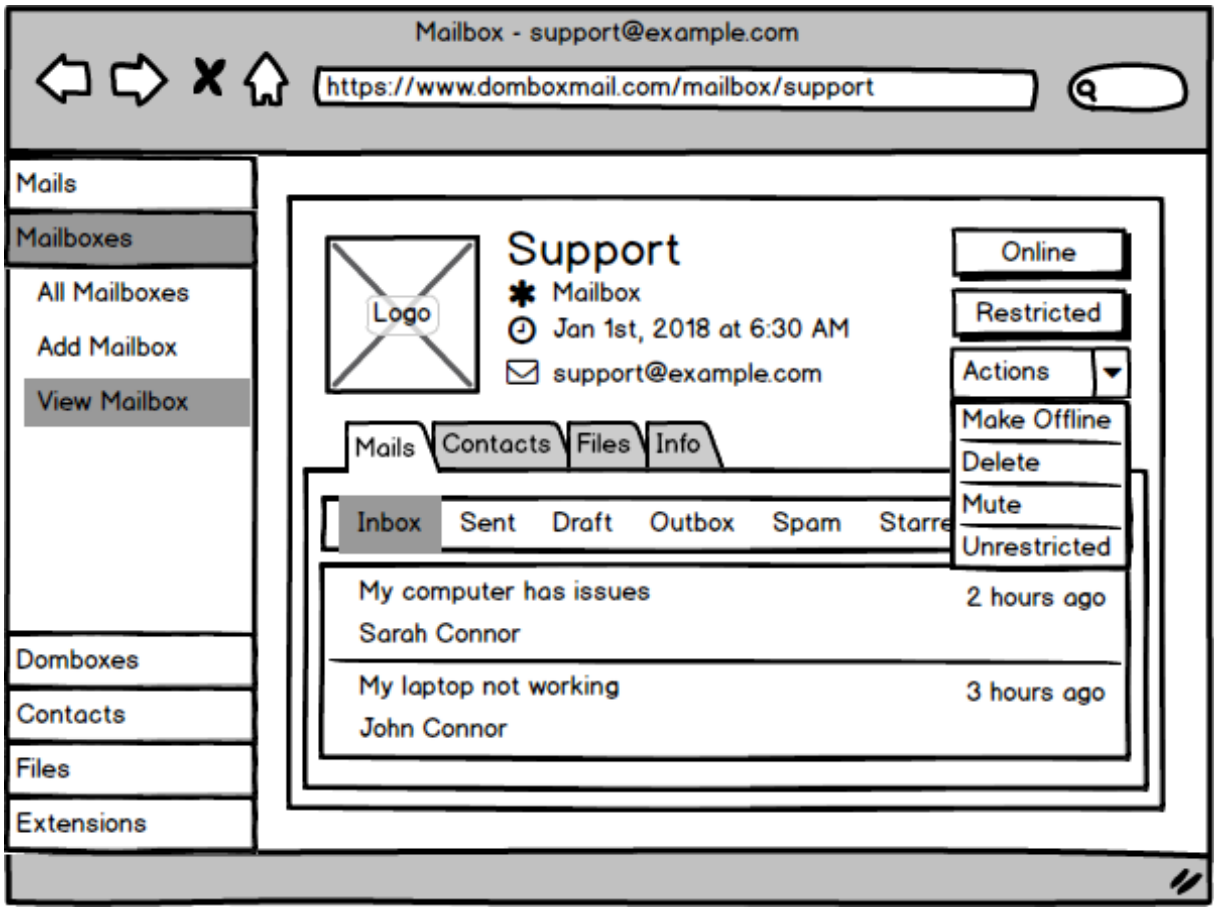


Figure 116: Restricted Box

This mode applicable only for the boxes found in “Mailboxes” group

But you can use this mode only when you have “Domboxes” extension enabled.

So this option is for “Mailboxes”, but you need “Domboxes” to use this feature.

“Restriction” is a subprocess of “Isolation”. In other words, without Isolation, you cannot have Restriction.

Whatever we did so far, mail classifications, isolation etc, we did just to have this “Restriction” phase.

The idea is that you are actually offloading all website related mails (i.e. Promotional Mails

and Transactional Mails) to the Domboxes. So only Conversational mails are what's left in Mailboxes.

You can find most of your "Conversational Mails" contacts in your "Address Book". So when you enable "Restricted Mode", you are asking us to allow emails only from the contacts found in your "Address Book".

Restricted Mode is an optional feature. By default, it's turned off. You need to enable it to use that feature.

When you enable "Restricted Mode" for the first time, you must agree to our "Restricted Mode" terms. e.g. You must use that box only for "Conversational Mails" after you enable "Restricted Mode".

You can turn on/turn off this mode anytime.

When it's turned off, it allows emails from everyone. But not from the "Blacklisted" contacts

When it's turned on, it allows emails only from the "Whitelisted" and "Neutral" contacts. For all others "Injection" rules apply. {Refer next chapter}

If you send an email to a new contact, it will be automatically whitelisted.

If you ever deactivate the Domboxes extension, then the restricted mode will be deactivated too.

Warning Text

When you enable "Restricted Mode", the warning text would look something like this.

> Caution:
>
> You are about to enter a sensitive zone.
>
> "Restricted Mode" is intended for the boxes that deals with only conversational mails. So offload all website related mails to the Domboxes before you enable this mode.
>
> When the Restricted Mode is ON, we will send a challenge mail to the Sender if the

> sender is not found in your “Address Book”.
>
> Real users can respond to those challenges. e.g. CAPTCHA. But automated and bulk mailers cannot. So their mails **never** gonna reach your inbox when the box is Restricted.
>
> Do you understand what you are signing up for?
>
> (a) Yes, I know what I’m doing
>
> (b) No, Get me out of here.

Users need to accept our “Restricted Mode” terms and condition before enabling that. They have to agree that the box will be used only for “Conversational Mails” and our company takes no responsibility if “website related mails” missing when sent to that box.

Greylisted Mode

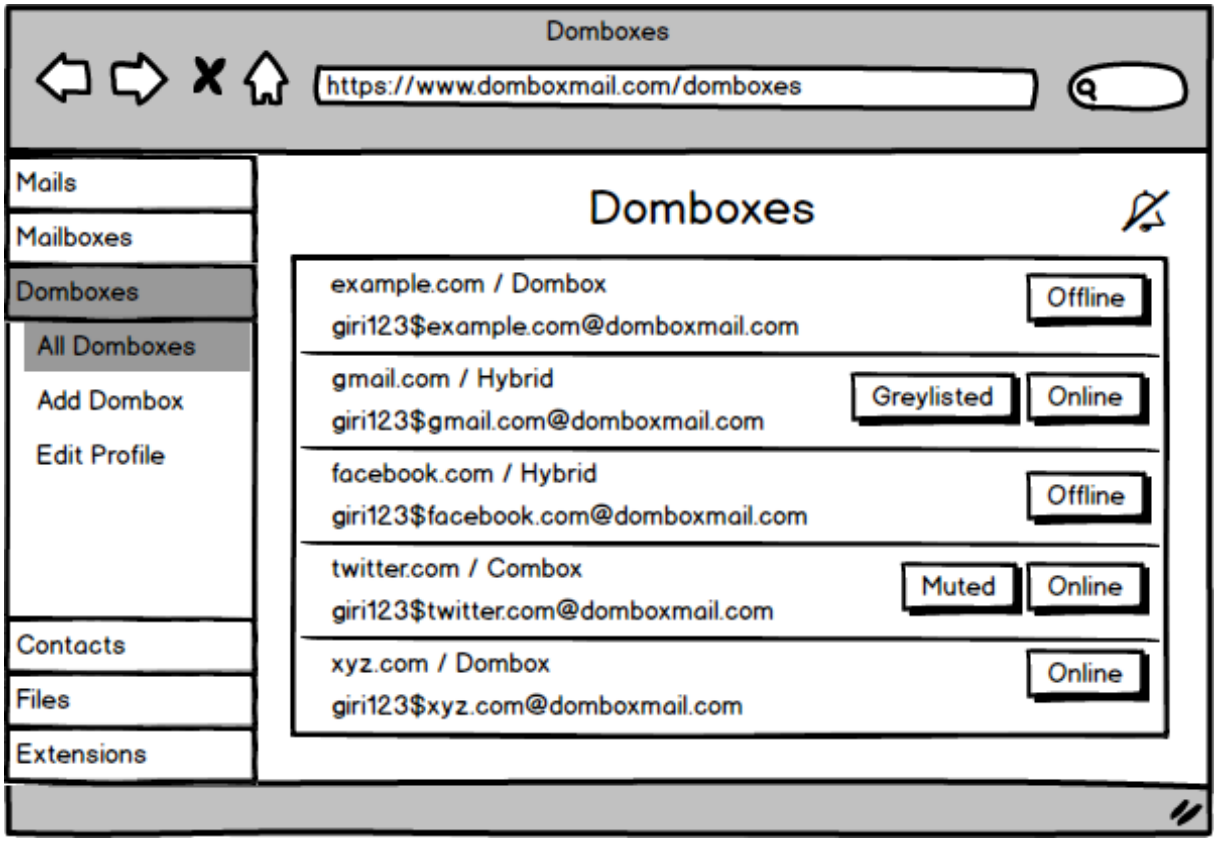


Figure 117: Greylisted Mode - List View

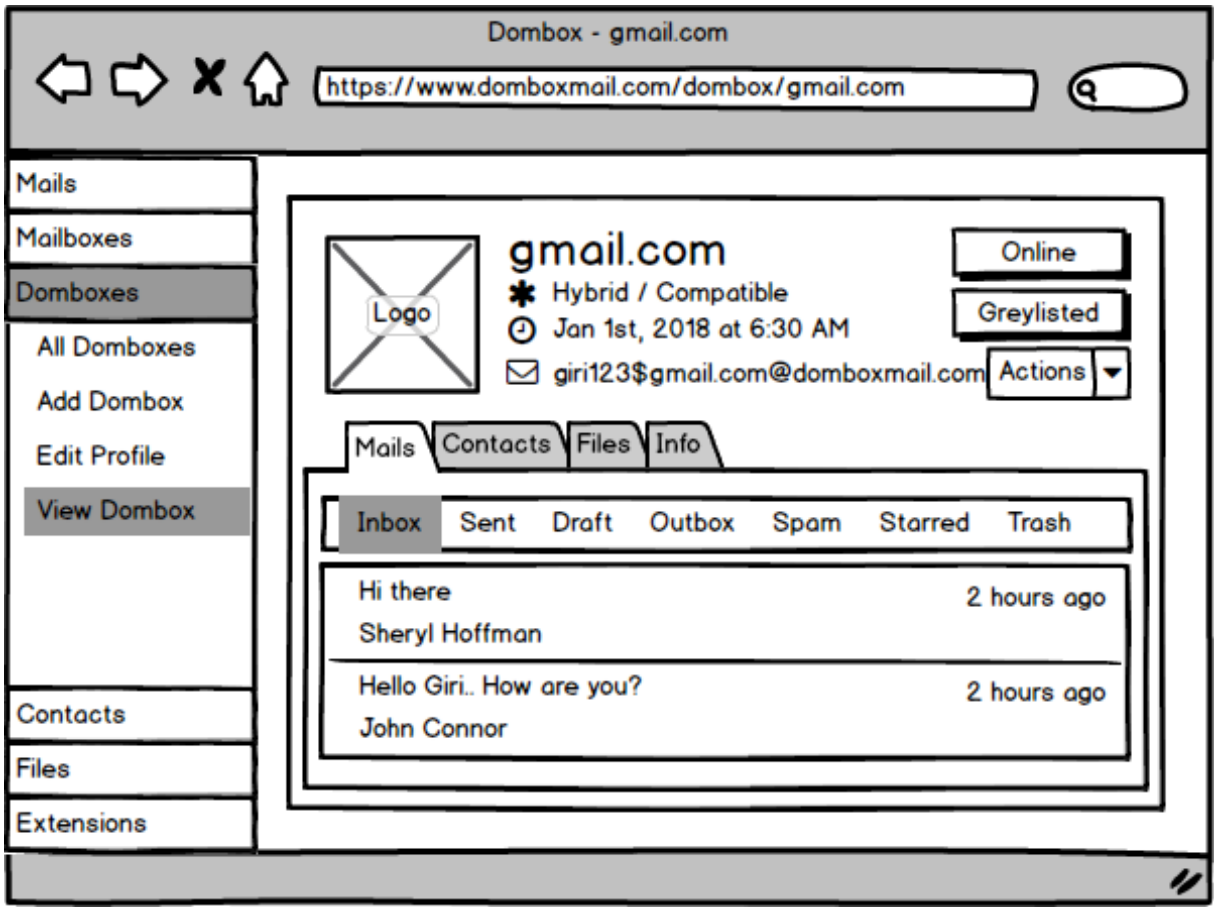


Figure 118: Greylisted Box

This mode applicable only for the boxes found in “Domboxes” group

This mode applicable only for certain boxes in “Domboxes” group.

Same “Restricted Mode” rules apply with few exceptions

Domboxes are Domain-based isolated mailboxes and it usually verifies whether the sender domain is authorized to send emails for the “Dombox Domain”.

Since we are verifying only the domain and not its users, there is a possibility where spammer use free mail services like gmail.com to send out spam.

For example, the consumer “Giri” creates a Dombox for gmail.com and give it to the user

John Doe who has email address john@gmail.com.

Jane Smith is a spammer who also has a free Gmail account jane@gmail.com.

Jane Smith can now send spam to Giri's gmail.com Dombox.

Just like "Restricted" mode, all incoming emails are restricted to "Address Book" in "Greylisted" mode too. Only the people found in the "Address Book" are allowed to send emails to the consumer.

However, for "Greylisted" mode, only the Dombox Domain's contacts (i.e. @gmail.com in this case) are allowed whereas in "Restricted" mode all contacts are allowed.

"Greylisted" mode applicable only for the popular mail services where anyone can signup and send emails.

"Greylisted" mode automatically enabled when the consumer creates a "Dombox" for free mail service domains like @gmail.com, @yahoo.com, @outlook.com, @domboxmail.com etc.

Note for website owners: If a greylisted domain is found in your SAD record, then we won't consider that as valid SAD domain

e.g "v=sad1 gmail.com:r+b example.com:s -all"

In the above case, only example.com is considered as a valid SAD domain.

Mails from gmail.com will be rejected in your domain's dombox.

Chapter 16: Injection

Finally, Let's talk about "Injection" part.

Although we made our system bulletproof from spammers via "Isolation" and "Restriction", we also made our system bulletproof from "Genuine Unknown Senders". So we need to improve the system.

This phase only deals with "Strangers". This phase makes sure only the "Genuine Unknown Senders" can able to mail you without any issues. But not the spammers.

This phase contains a few methods. But the one that would work for everyone is the CAPTCHA method.

So, We are gonna send an email back asking the sender to fill CAPTCHA. This type of system is known as Challenge/Response mechanism and it was first introduced in 1997.

Let's see the available methods.

Method 1: Intro via a Mutual Contact

Task Performed By: Mutual Contact

Estimated Burden: ~ 1 Minute / Automatic during a conversation

Let us give you a Quick Primer about Recipient Mail Headers.

You can add the mail recipient in one of the following three ways. To, CC, BCC

Header	Description
To	Main Recipients. e.g. A Project Team Members
CC	Carbon Copy. Observers. They don't have to participate in the conversation. i.e. They don't have to add any reply. e.g. Your Boss or the Project Manager / Supervisor.
BCC	Blind Carbon Copy. Secret Observers. Both To and CC members never aware of BCC.

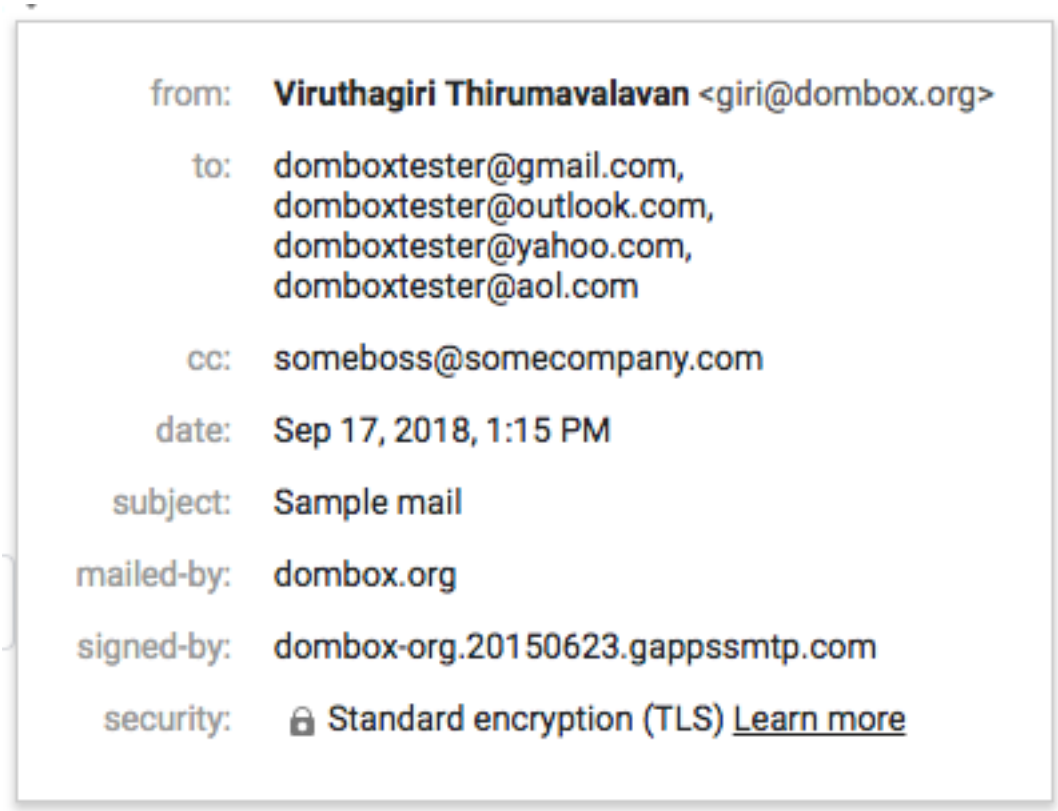
Example:

> From: giri@dombox.org
>
> To: domboxtester@gmail.com, domboxtester@outlook.com, domboxtester@yahoo.com, domboxtester@aol.com
>
> CC: someboss@somecompany.com

> BCC: someotherboss@somecompany.com

Let's send that mail to domboxtester@gmail.com

This is how it looks when the mail viewed by domboxtester@gmail.com



Just think of domboxtester@gmail.com as a "Restricted Box" and giri@dombox.org is a whitelisted contact in that box.

So giri@dombox.org can mail to domboxtester@gmail.com without any issues. Because that contact is trusted by the receiver.

Chain of Trust

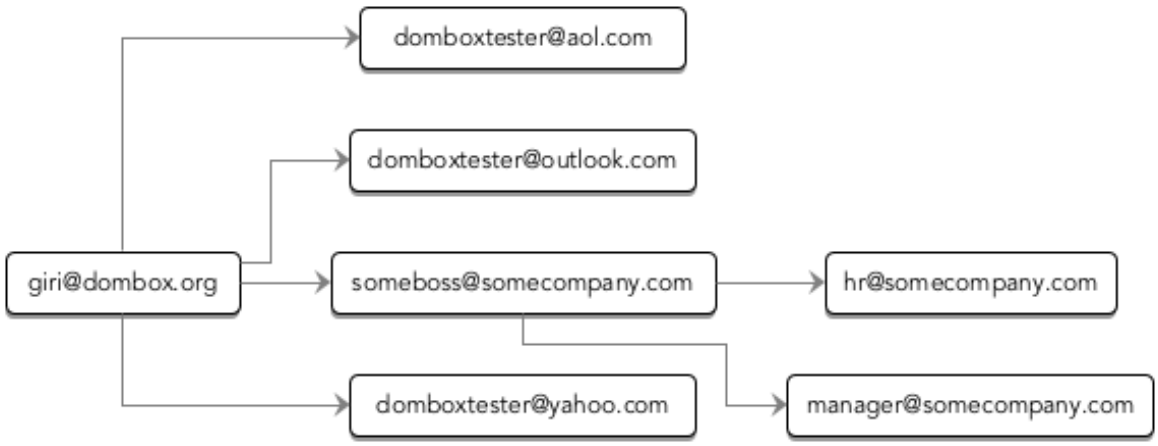
From the domboxtester@gmail.com perspective, the following 4 contacts are "never before seen" contacts.

domboxtester@outlook.com, domboxtester@yahoo.com, domboxtester@aol.com, someboss@somecompany.com

But since it's actually introduced via a trusted contact giri@dombox.org, we are gonna trust these 4 email addresses.

Let's say someboss@somecompany.com introduces two more "never before seen" contacts. manager@somecompany.com, hr@somecompany.com

The chain would look like this.



We cannot keep going forever on the chain. So we should have a maximum limit for the depth. e.g. 5 {Think of it like a nested comment system. There should be a limit in the depth.}

In the last figure, giri@dombox.org is a trusted contact. But domboxtester@outlook.com, domboxtester@yahoo.com, domboxtester@aol.com and someboss@somecompany.com are nothing but "Level 1 Guests" until those contacts moved to the "Address Book" by the receiver / owner.

manager@somecompany.com and hr@somecompany.com are "Level 2 Guests".

We should have a list called "Guest List". Contacts found in the "Guest list" should have limited privileges. e.g. Limit number of mails that can be accepted from that contact in a day, Limit number of contacts that can be introduced via that contact etc.

The receiver / owner should be able to move the contact from "Guest List" to the "Address Book".

The system automatically detects and whitelist the Guests when "Restricted Mode" en-

abled. So if you are already participating in a mail conversation via a mutual contact, you don't have to ask the "mutual contact" to introduce you again.

But if you never participated in any conversation and you know a mutual contact, then ask that person to send a mail like this from his account.

> From: mutualcontact@gmail.com
>
> To: giri@dombox.org
>
> CC: johndoe@gmail.com
>
> Sub: Introduction
>
> Message:
>
> Hey Giri,
>
> John is a good friend of mine and he would like to connect with you.
>
> Regards,
>
> Mutual Contact.

Method 2: CAPTCHA

Task Performed By: Sender

Estimated Burden: ~ 1 Minute

This method works exactly like Google reCAPTCHA. The idea is that spammers usually send millions of mails. They don't have enough time to manually enter the CAPTCHA.

Since we already isolated the website mails, websites don't have to worry about entering the CAPTCHA.

Note: All Injection methods are applicable only for "Normal Mailboxes i.e. Conversational Mails". Bulk mailers gonna have problems. But Genuine Unknown Senders not gonna have any problem in entering those CAPTCHA.

If your business relies on sending bulk mails, make sure to force your users to create an

"Isolated Mailbox" for your domain instead of just accepting "Normal Mailbox". This is the primary reason why we have "Domboxes".

Method 3: Phone Number Validation

Task Performed By: Sender

Estimated Burden: ~ 1 Minute

In this method, the sender needs to enter your phone number correctly.

People who have your "Phone Number" could be the people you once met and gave your business card. The phone number acts like a PIN number here. A spammer may have your email address but not your phone number.

Method 4: Proof-of-Work (PoW)

Hashcash[71] is the first Proof-Of-Work (PoW) method and it was invented by Adam Back in 1997[72].

Put it this way, What CAPTCHA is for humans, Proof-of-Work is for computers.

The idea is that, a computer need to solve a puzzle by giving up some computer processing power. Let's just say it takes 10 seconds to solve this puzzle. This is perfectly fine for Genuine senders who send few mails a day. But not for spammers who send millions of spam mails.

This is how a hashcash header would look like in email.

> From: Someone <test@test.invalid>
>
> To: Adam Back <adam@cypherspace.org>
>
> Subject: test hashcash
>
> Date: Thu, 26 Jun 2003 11:59:59 +0000

[71] https://en.wikipedia.org/wiki/Hashcash
[72] http://www.hashcash.org/papers/announce.txt

> X-Hashcash: 0:030626:adam@cypherspace.org:6470e06d773e05a8
>
> blah blah
>
> -Someone

The receiving server need to extract the X-Hashcash header and then verify the Hashcash.

Today we have a much better decentralized and distributed Proof-of-Work system like Blockchain. In fact, Blockchain is the successor of Hashcash. Bitcoin is one of the most famous application written on top of Blockchain.

In our solution, Proof-of-Work is just a replacement for the Challenge/Response mechanism like CAPTCHA. You still need to be a verified stranger for the mail to be accepted in Mailboxes (i.e. Conversational Mail). The term “Verified Stranger” will be explained in a later section.

For CAPTCHA method, (1) we receive a mail from verified stranger (2) We send a challenge mail back (3) We receive a response for the challenge. So three steps Receive, Send and Receive. In Proof-of-Work, the challenge is already completed by the sender before even sending the mail. So it’s only one step.

PoW methods like Hashcash are vulnerable to BotNets since the botmaster doesn’t care about wasting their victim computer processing power. In our system PoW methods are safe from BotNets. Refer the section “Verified Strangers” for more info.

Method 5: Attention Fee

Task Performed By: Sender

Estimated Burden: ~ 3 Minutes

When it comes to the Internet, it’s all about getting your attention.

Spammers are no different from them. They are here for your attention too. They succeed even if you open an email and read it for a couple of seconds.

The way we see it, if you receive 1000 emails in a year, 900 (90%) of them will be Transactional and Promotional Mails.

100 (10%) of them will be Conversational mails

If we dissect those 100 Conversational Mails, 90 of them would be from known people and 10 of them of would be from unknown people (Note: We are assuming you are an average internet user here.)

90 (90%) of them would be from known people (We fixed this with Restricted Mode)

10 (10%) of them would be from Unknown people (This is where we need injection methods like CAPTCHA)

The “Attention Fee” will be set by the “Receiver”. The money can be from 1 cent to $1000. The default will be 1 cent. If you are not a busy person like Bill Gates, you should go with a low value.

If you set a very high value, then even genuine people can’t able to contact you. You are trying to fight spammers here. Not scare genuine people.

The “Attention Fee” will be charged from the sender, before sending it to the receiver. If the mail is marked as “Genuine” by the receiver, then the money will be returned back to the sender and the contact will be whitelisted.

Our “Attention Fee” model is similar to the system Bill Gates and his team designed back in 2004 to fight spammers. It didn’t work for them at that time. But it will definitely work in ours.

This is because Mr. Gates applied “Payment Model” for all mails including Transactional and Promotional mails. In our system “Payment Model” is applicable only for Conversational Mails and that too only for “Strangers”.

Payment mode was their “Primary” line of defense. In our case it’s “Tertiary” i.e. Isolation => Restriction => Injection. Note: Injection is a sub phase of Restriction. And Restriction is a sub phase of Isolation. In other words, You can’t have “Injection” without “Isolation and Restriction”.

And all three phases are optional. Meaning you can only use the Normal Mailboxes just like Gmail. i.e. The traditional way

Attention Fee Calculation

The default value is 1 cent. But the default value is not an optimal value if you are a busy person

For example, If you are Bill Gates or Jeff Bezos then 1 cent is definitely not an Optimal value

So, here are the steps to calculate your attention fee

Step 1: Take your annual salary (e.g. Dave is a Software Engineer in San Francisco who makes $200,000 USD annually)

Step 2: Divide your salary by 2000. That's your hourly pay. In Dave's case, it's $100

Step 3: Multiply your hourly rate by 100 to get the value in cents. In Dave's case, it's 10,000

Step 4: Divide that "Cents" value by 3600. That's how much you make per second. In Dave's case it's 10000 / 3600 = 2.77

Step 5: So Dave's 1 second is worth 3 cents.

Step 6: You are going to spend at least 5 seconds in opening, reading and deleting the spam mail. So multiply by 5. In Dave's case its 15 cents

That should be the minimum suggested value you should charge for attention fee.

Of course, you are welcome to multiply that value by any number or you can just leave it to the default value "1 cent". It's up to you.

Bounce Address

When an email cannot be delivered, the MTA will create a bounce message and send it to the address given by the MAIL FROM command.

The email address provided by the MAIL FROM command is also known as Envelope From, Envelope Sender, Return Path, Reverse Path, RFC.5321 From and Bounce

Address[73].

This whitepaper heavily uses the terms MAIL FROM and Envelope From. Both refers to the same thing.

Bulk Mailers Bounce Address

When a website sends you promotional mails they are running a campaign. They need to know whether it's delivered or not.

So the Bounce Address (i.e. Envelope From Email Address) will be uniquely generated for that campaign and user when bulk mailers mailing you. Refer the term "Variable Envelope Return Path[74]"

Example: DigitalOcean

Type	Address
Bounce Address (aka. Envelope From)	bounce-md_30039865.5b4fba9d.v1-c350d739e302497090f1b86169e7f63f@mda.digitalocean.com
Message From	support@support.digitalocean.com

Example: CloudFlare

Type	Address
Bounce Address (aka. Envelope From)	bounce-mc.us5_10559331.590349-giri=dombox.org@mail61.atl91.mcsv.net
Message From	cfmarketing@cloudflare.com

As you can see, it's quite normal to have different email address for "Envelope From" and "Message From" when websites send you bulk mails.

[73] https://en.wikipedia.org/wiki/Bounce_address
[74] https://en.wikipedia.org/wiki/Variable_envelope_return_path

Conversational Mails Bounce Address

In Bulk Mailers case, there is gonna be millions of users like you. So they have a unique bounce address for each user.

In our Cloudflare example, it uses MailChimp to send out those bulk mails. So MailChimp uses its domain mcsv.net for the "Envelope From". So even a completely different domain is normal here.

When we mean Conversational Mails we are talking about Mailboxes on both sides. However, In Bulk Mailers case, we are talking about Mailboxes on only one side.

In Conversational Mails, when a mail not gets delivered, you want the non-delivery report gets delivered to the person who mailed you. So both "Envelope From" and "Message From" gonna be the same for Conversational Mails most of the times.

Example:

Type	Address
Bounce Address (aka. Envelope From)	giri@dombox.org
Message From	giri@dombox.org

Display Address

In some cases "Envelope From" and "Message From" will be different in Conversational Mails.

e.g. When you use "Send mail as" feature found in Gmail, your "Message From" address will be the value you set, but "Envelope From" will be your original gmail address.

Gmail => Settings => Accounts => Send mail as

Example:

Original Mail address: domboxtester@gmail.com

Send Mail as: giri@dombox.org

Type	Address
Bounce Address (aka. Envelope From)	domboxtester@gmail.com
Message From	giri@dombox.org

The most important point you have to note here is that “Envelope From” will always be an email address that can “accept” replies and read by a “Human” in “Conversational Mails”. So this human can able to respond to our challenge mails.

Challenge Mail

This is how our challenge mail would look like.

> From: challenge@dombox.org
>
> To: someuser@gmail.com
>
> Sub: Mail Delivery Pending
>
> Message:
>
> The following recipients enabled Restricted Mode[a].
>
> user1@domboxmail.com
>
> user2@domboxmail.com
>
> user10@domboxmail.com
>
> And your contact not found in the recipient Address Book.
>
> Please verify that you are human by filling the CAPTCHA in the following link to deliver the mail.
>
> http://www.domboxmail.com/challenge/abcde/fghij

> Our apologies for the inconvenience.
>
> [a] http://www.domboxmail.com/mailboxes/help/restricted

Challenge Form

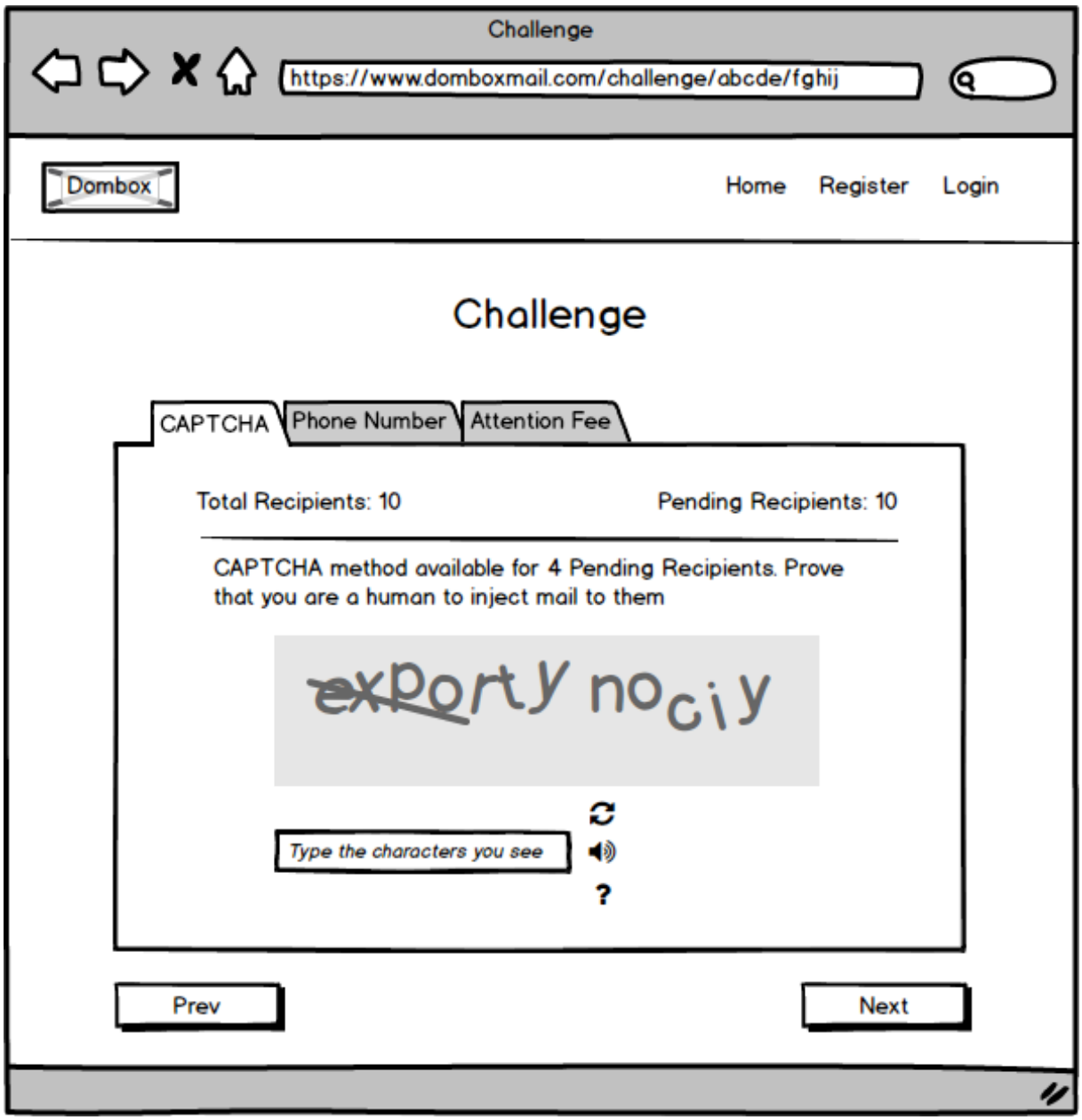


Figure 119: CAPTCHA Challenge

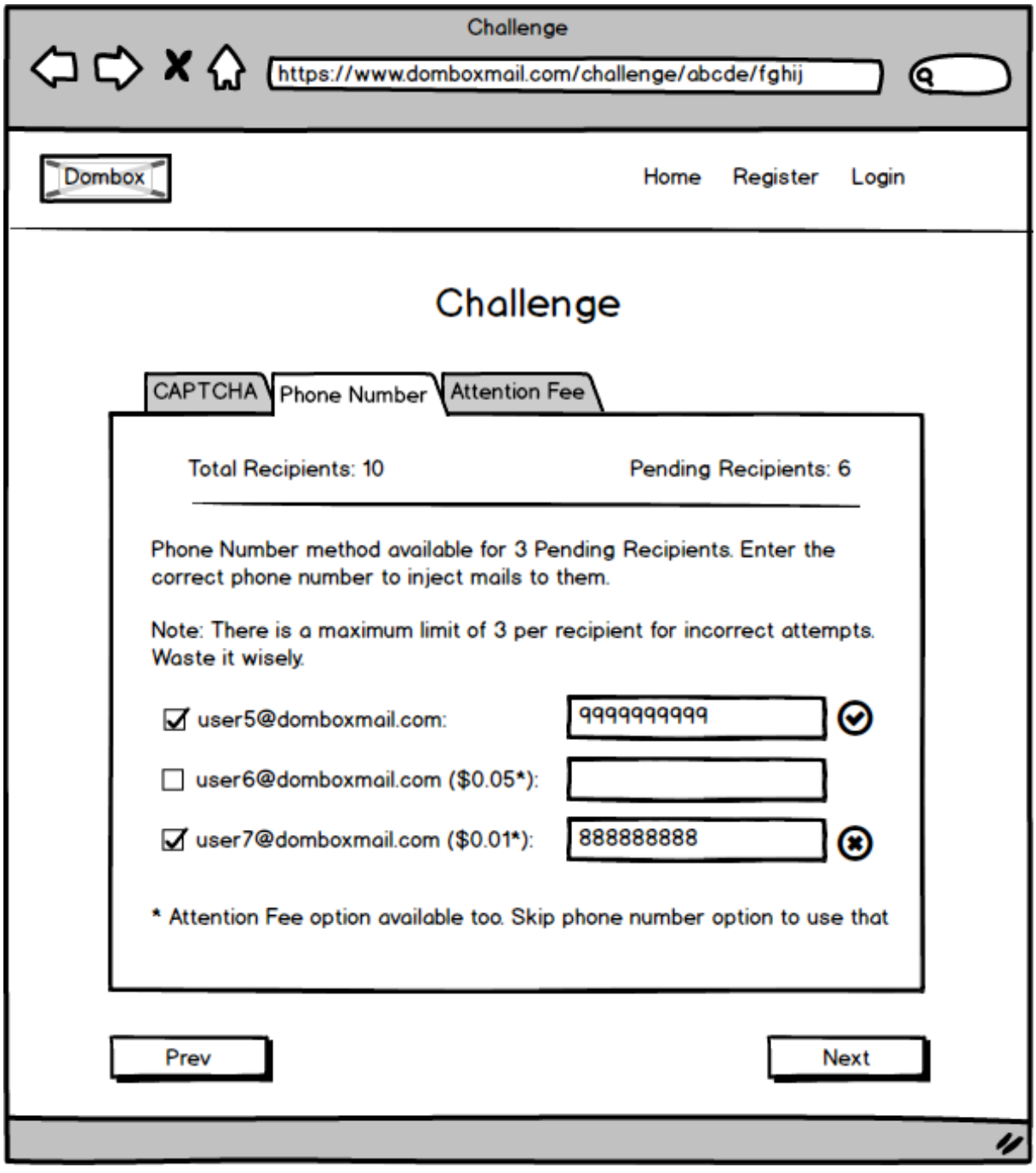


Figure 120: Phone Number Validation

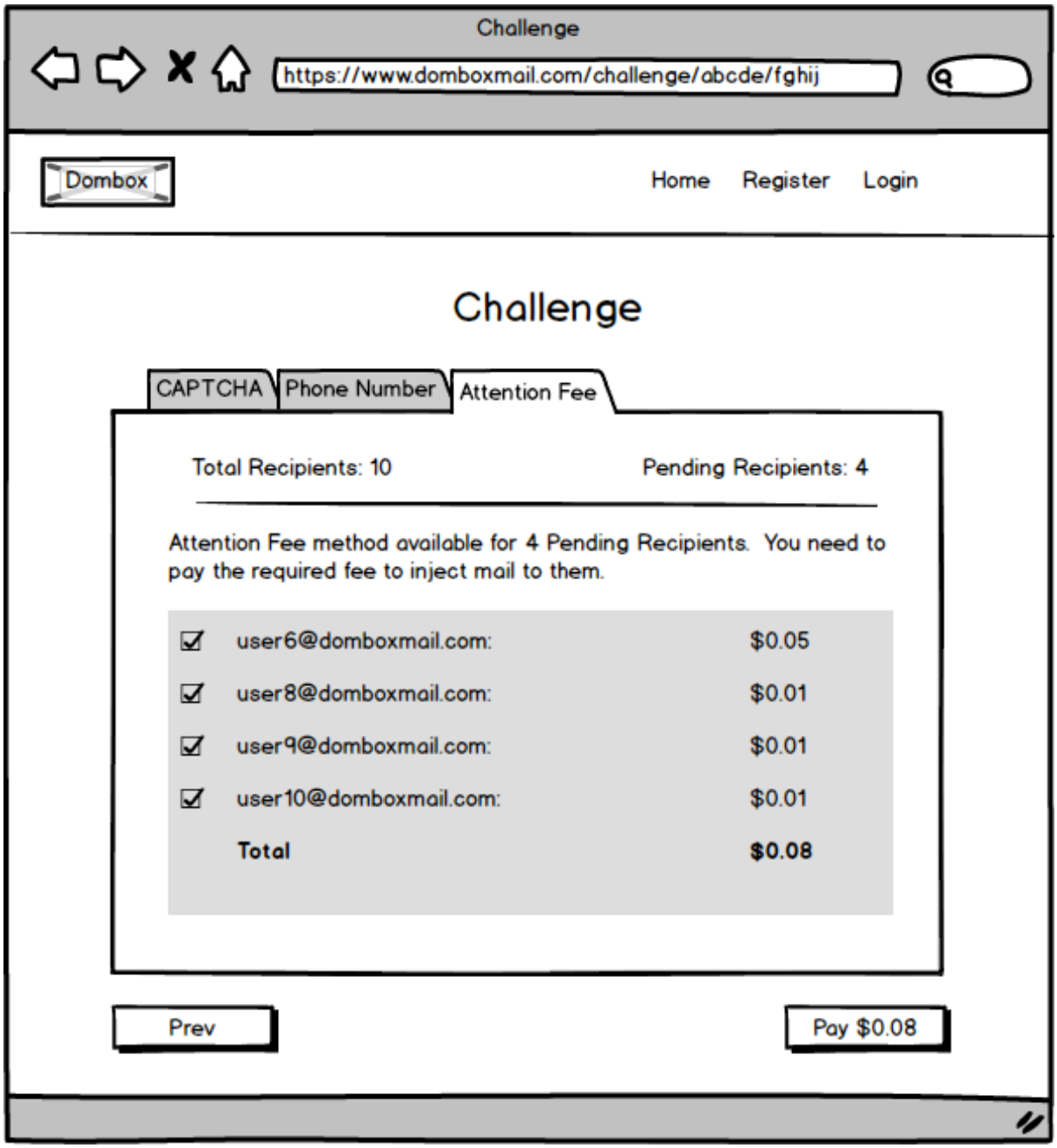


Figure 121: Attention Fee

Non-Delivery Reports

Let's go over our sample SMTP chat one more time.

> mail.example.com Connecting to mail.domboxmail.com with its IP address
>
> domboxmail.com => 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> example.com => HELO mail.example.com
>
> domboxmail.com => 250 Hello, nice to meet you, mail.example.com
>
> example.com => MAIL FROM: <john@example.com>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <user1@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <user2@domboxmail.com>
>
> domboxmail.com => 550 Invalid Recipient
>
> example.com => RCPT TO: <user3@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <user4@domboxmail.com>
>
> domboxmail.com => 550 Mailbox Full
>
> example.com => RCPT TO: <user5@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => DATA
>
> domboxmail.com => 354 End data with <CRLF>.<CRLF>
>
> {Message Part goes here}
>
> domboxmail.com => 250 OK, message accepted for delivery: queued as 12345
>
> example.com => QUIT

> domboxmail.com => 221 Bye

In the last SMTP Conversation, we have 5 RCPT TO commands. The mail is rejected for user2 and user4. But for all other users, the mail is accepted.

For each RCPT TO command, we have to make sure the recipient address exists on our system. If the recipient address has no issues we are gonna respond with 250 code. If there is an issue, we are gonna respond with an error code saying we can't accept mail for that user.

If we get past RCPT TO without rejecting the mail and if there is an issue, then we have to either reject the mail for all recipients or send an email back to the sender saying there is an issue with particular recipients (user2 and user4 in our case) . This is known as bounce message.

Backscatter Attacks

Email can be easily forged.

If a mail we receive says "president@whitehouse.gov", that's not always gonna be true. If we keep sending bounce messages or challenge mails to "president@whitehouse.gov", then we have a far more serious problem.

So non-delivery reports during the SMTP conversation are much more safe than sending bounce mails.

As for Challenge Mails, we need to make sure mails from "Strangers i.e. unknown senders" are not forged.

Sender Policy Framework

SPF is one of the best mechanisms we have for email to detect email spoofing. We compare the "Incoming mail IP address i.e. Client IP" with the whitelisted IP addresses found in the SPF records.

For example this is the SPF record of facebook.com

```
GiriMac:Prototype giri$ dig +short txt facebook.com
"v=spf1 redirect=_spf.facebook.com"
GiriMac:Prototype giri$ dig +short txt _spf.facebook.com
"v=spf1 ip4:69.63.179.25 ip4:69.63.178.128/25 ip4:69.63.184.0/25 ip4:66.220.144.128/25 ip4:66.220.155.0/24
 ip4:69.171.232.0/24 i" "p4:66.220.157.0/25 ip4:69.171.244.0/24 mx -all"
GiriMac:Prototype giri$
```

Figure 122: SPF Query

But there is one bigger problem with SPF. It's an optional mechanism. i.e. There is no internet standard that says, a domain MUST configure SPF.

The popularity of SPF record fades away once we get past the alexa top 1 million domains. So if we rely only on SPF record, then the solution may work for the 100th domain, but not gonna work for the 100 millionth domain.

Hot Gates Strategy

Have you ever watched the Gerard Butler starred movie 300? If yes, let us ask you a question?

Figure 123: Hot Gates

In that movie, King Leonidas and his soldiers battle against 300,000 persian soldiers, near a narrow pass called “Thermopylae aka. Hot Gates”.

Our question is, Why Hot Gates? Why not battle in an open ground?

That’s because these spartans strength not only lies on their superior fighting skills, but also lies on their tactical advantage. Without “Hot Gates”, the whole battle would have been an instant massacre.

Challenge/Response mechanism is a weapon that should be used in a narrow battle like “Hot Gates”. But every C/R based spam solution out there, trying to use the C/R mechanism in an open ground battle. That is the main reason why C/R mechanism is flawed and not popular even though it got patented[75] 20 years back.

Email is ubiquitous. You know what else is ubiquitous?

MX Records. They were introduced in 1986.

Let’s refresh our memories.

- We classified the mails into three categories. Conversational Mails, Transactional Mails and Promotional Mails.
- We offloaded Transactional Mails and Promotional Mails to Domboxes.
- Users agree that they are gonna use the Mailboxes only for “Conversational Mails” when “Restricted Mode” is ON.

So... In “Injection” phase, we are dealing with only “Strangers”. Not just any strangers. We are talking about “Conversational Mail Strangers”. Context really matters here.

We already gave unrestricted access to websites and apps in Domboxes via “Isolation”. So, there is no such thing as “Transactional Mail Strangers” or “Promotional Mail Strangers” in our system.

The term “Conversational Mails” can be termed as MX-to-MX Mails.

e.g. When john@example.com sends an email to jane@gmail.com, Gmail.com MX record is queried and then mail will be transferred to one of the Gmail MX servers. When Jane reply to that mail, example.com MX record is queried and then mail will be transferred to

[75] https://patents.google.com/patent/US6199102B1/en

one of the example.com MX servers. So Conversational Mails requires MX record on both sides.

So “MX Records” should be the “Hot Gates” of our Challenge/Response based email system. i.e. We actually diverted the spammers to the injection phase by Isolating and Restricting the genuine senders.

Our primary clue for verifying mail genuineness now is “MX Records”. Let’s verify these stranger mails.

MX Records

This MX Record check is part of our Authorization Layer check.

Self-Hosted

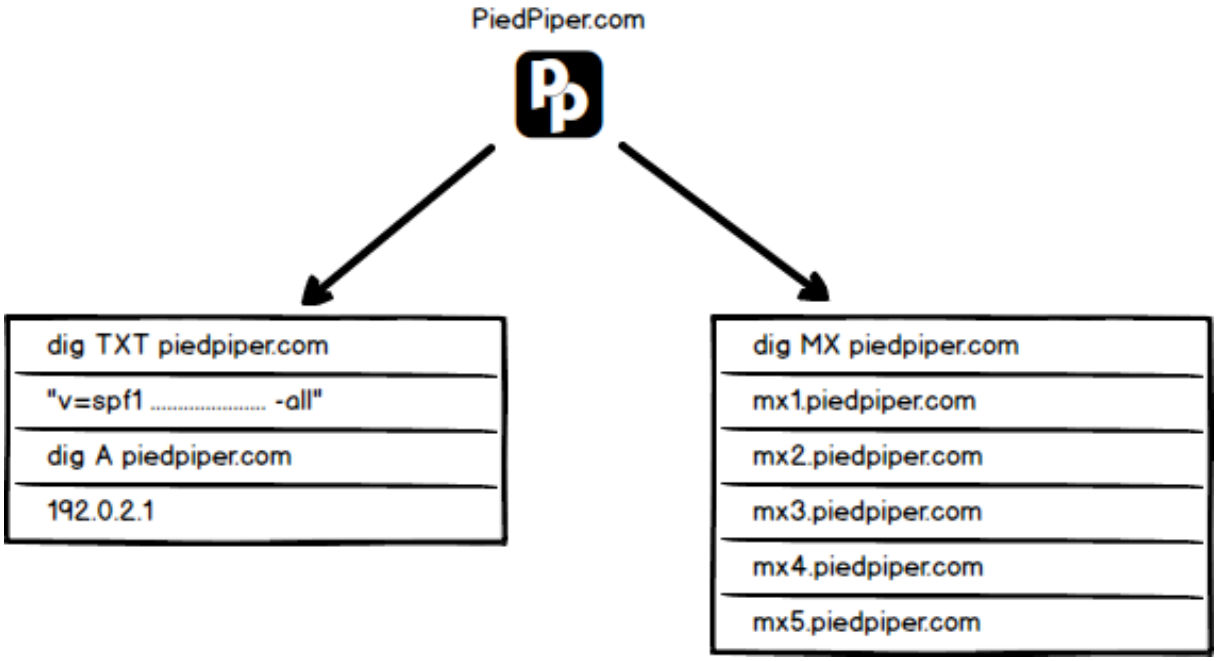


Figure 124: Self-Hosted

When a mail coming from richard@piedpiper.com, we are gonna compare the “Incoming mail IP i.e. Client IP” address with the IP addresses extracted from the following records.

dig MX piedpiper.com (MX Records)

dig TXT piedpiper.com (SPF Record)

dig A piedpiper.com (A Record)

Third-Party Hosted

When MX server domain not ends with the same domain, then that domain will be considered as a third-party hosted domain.

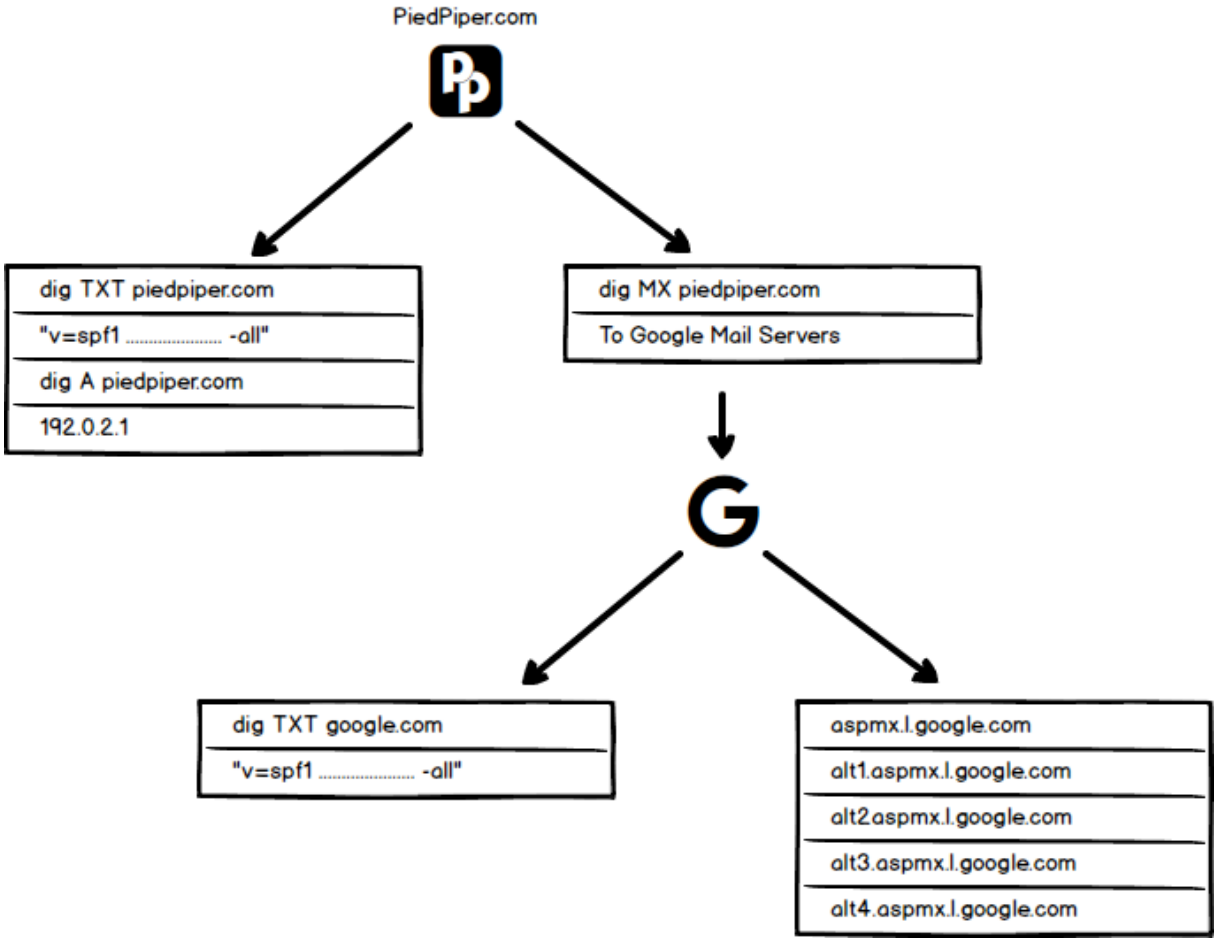


Figure 125: Third-Party Hosted

In this case, piedpiper.com hosting their mails in Google servers.

So we are gonna compare the “Incoming mail IP i.e. Client IP” address with the IP addresses extracted from the following records.

dig MX piedpiper.com (MX Records Points to google.com)

dig TXT piedpiper.com (PiedPiper SPF Record)

dig TXT google.com (Google SPF Record - The base domain of MX host)

dig A piedpiper.com (A Record)

Strangers

Isolation phase for websites

Restriction phase for friends, family, colleagues and acquaintance (aka Authorized Personnel)

Injection phase for Strangers

So the whole Injection phase applicable only for Strangers. Also keep in mind, the term "Injection" comes into play only when "Restricted Mode" is ON.

Isolation => Restriction => Injection

We can classify the Strangers into two categories based on the MX Record check we performed in the last section.

Verified Strangers and Unverified Strangers

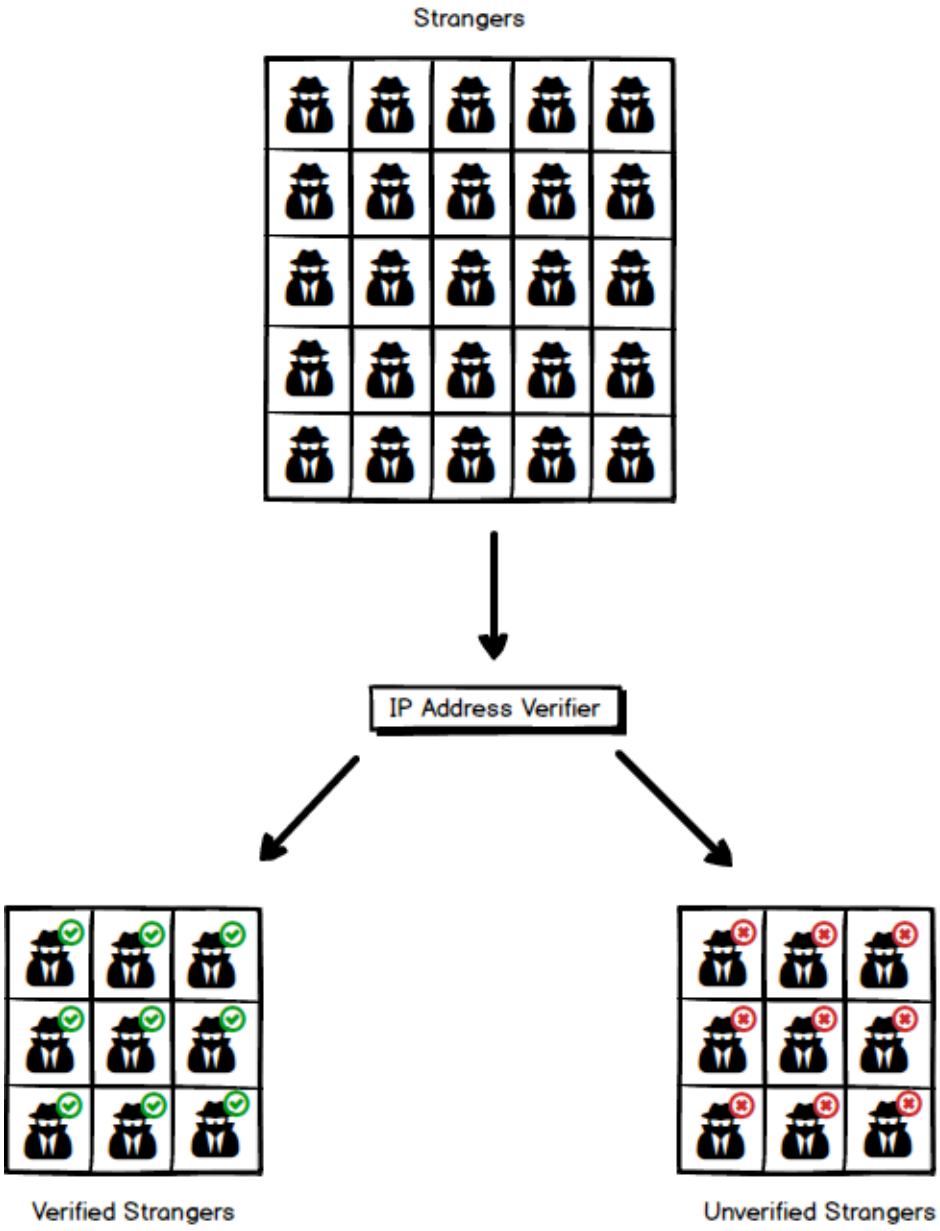


Figure 126: Strangers

Verified Strangers

Challenge/Response mechanism applicable only for verified strangers.

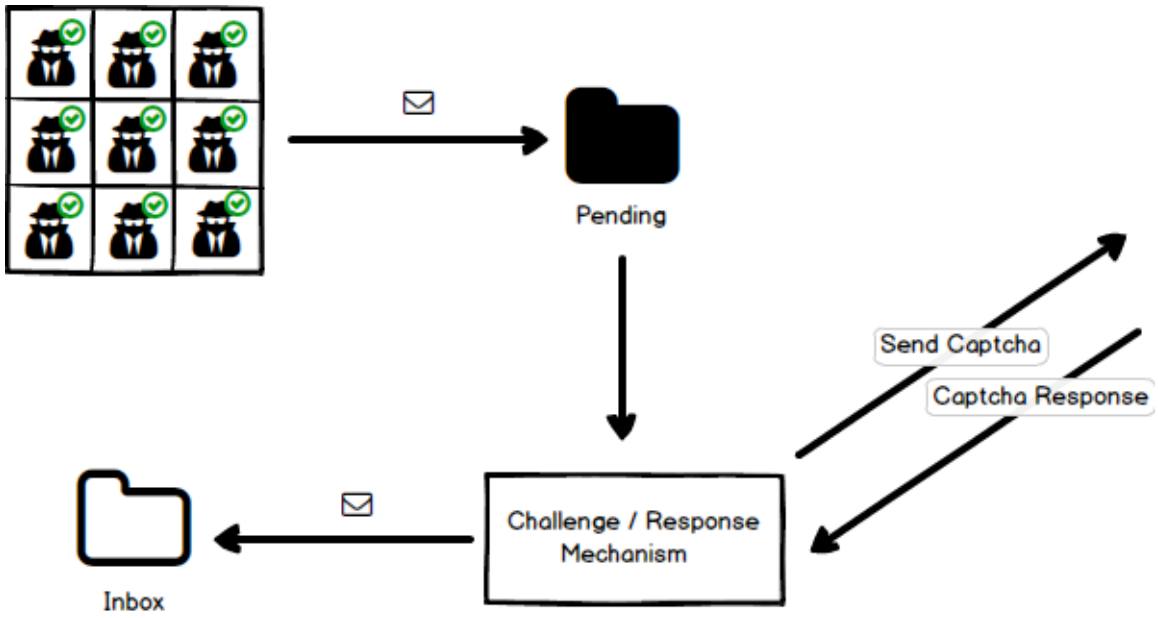


Figure 127: Verified Strangers

Here are the steps.

1. Accept the mails from “Verified Stranger” as usual.
2. Put the accepted mail in the“Pending” folder. Note: Users never can access the “Pending” folder. If we allow access to “Pending” folder, then it beats the purpose of the system since our “Pending” folder is a replacement for “Spam” folder.
3. Send the challenge mail to the “MAIL FROM” address.
4. If the sender complete the challenge and the response is valid, move the mail from “Pending” folder to the “Inbox” folder.
5. Discard the mail if it is “Pending” for more than 30 days. Most likely it is a spam mail since no one is ready to accept the challenge on the other side.

Unverified Strangers

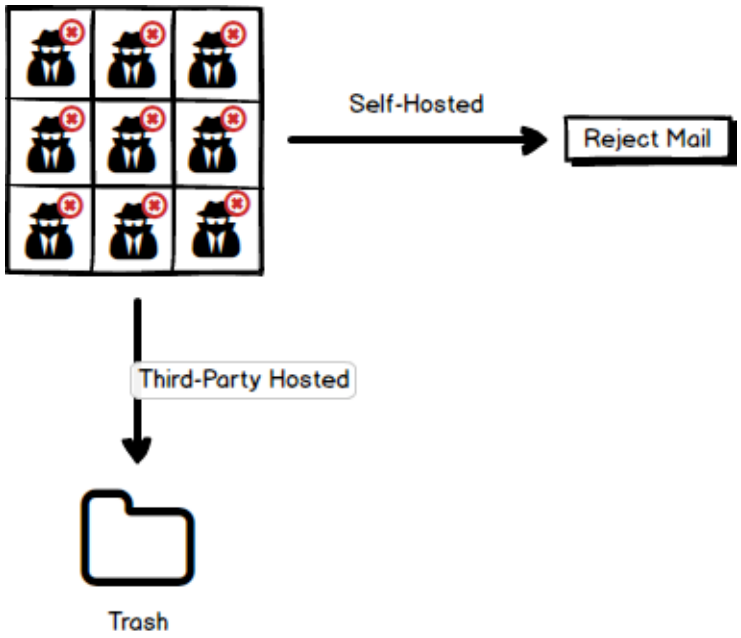


Figure 128: Unverified Strangers

Let's go over the Sample SMTP chat one more time.

> mail.example.com Connecting to mail.domboxmail.com with its IP address
>
> domboxmail.com => 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> example.com => HELO mail.example.com
>
> domboxmail.com => 250 Hello, nice to meet you, mail.example.com
>
> example.com => MAIL FROM: <john@example.com>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <user1@domboxmail.com>
>
> domboxmail.com => 250 OK

> example.com => RCPT TO: <user2@domboxmail.com>
>
> domboxmail.com => **550 Restricted Box. Unauthorized and Unverified Sender. Please configure SPF or Send this mail from one of your MX server IP address**
>
> example.com => RCPT TO: <user3@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <user4@domboxmail.com>
>
> domboxmail.com => **550 Restricted Box. Unauthorized and Unverified Sender. Please configure SPF or Send this mail from one of your MX server IP address**
>
> example.com => RCPT TO: <user5@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => DATA
>
> domboxmail.com => 354 End data with <CRLF>.<CRLF>
>
> {Message Part goes here}
>
> domboxmail.com => 250 OK, message accepted for delivery: queued as 12345
>
> example.com => QUIT
>
> domboxmail.com => 221 Bye

As you can see, we rejected mails for user2 and user4 with an error like this.

> **550 Restricted Box. Unauthorized and Unverified Sender. Please configure SPF or Send mail from one of your MX server IP address**

If the receiving domain is a Self-Hosted / Dombox-based system (e.g. @domboxmail.com), then the mails will be rejected with the following error.

550 Restricted Box. Unauthorized and Unverified Sender. Please configure SPF or Send this mail from one of your MX server IP address

If the receiving domain is a Third-Party Hosted / Mailbox-based system (e.g. @gmail.com),

then the mails will be moved to “Trash” folder instantly. {Refer next section for more info}

99.99% of the “Unverified Stranger” mails are from either spammers or probably the websites you didn’t want to isolate.

Genuine Senders rarely get caught here. If a genuine sender get caught here, then it’s actually their mistake. Put it this way, they have an address in America for incoming mails, but outgoing mails are originating from Japan. That’s abnormal since we are talking about “Conversational Mails” here.

Small businesses usually don’t go for such abnormal setup. Anyone who go for such abnormal setup probably doing that for better networking policies. These networking professionals most likely knew what is an SPF record.

Besides we are giving crystal clear error message when rejecting the mail.

This is how 550 error message would look like on the sender side when the mail gets rejected.

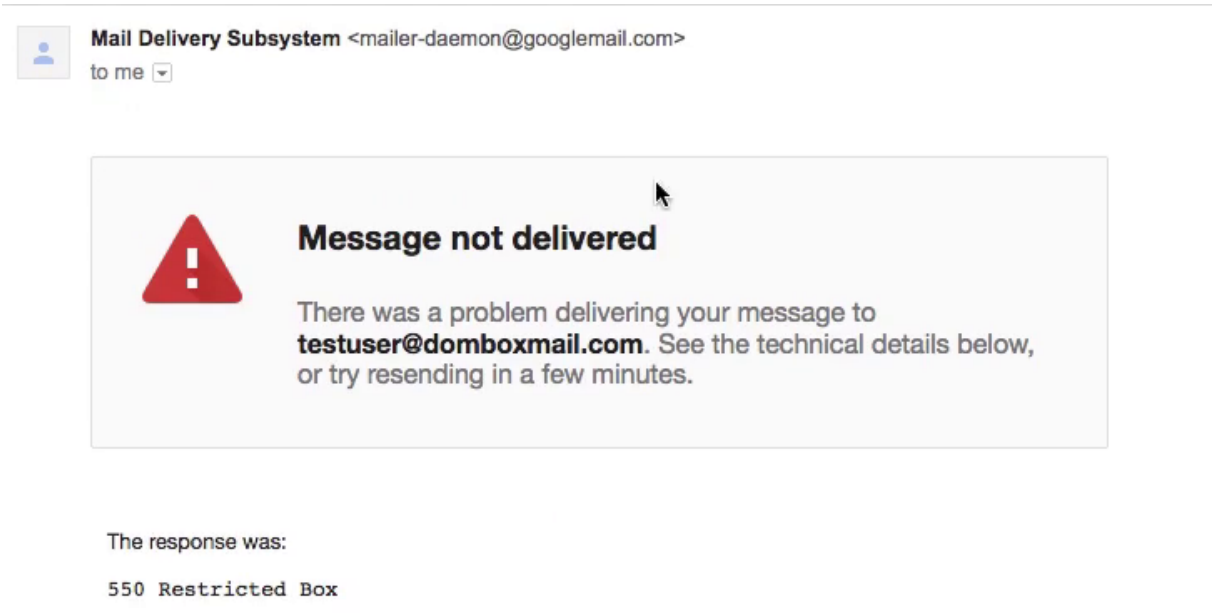


Figure 129: 550 Error Message

Domain Reputation

In Email 1.0, stranger reputation is tied to the IP address. As we mentioned earlier, Emails can be easily forged. If a spam mail says it's coming from "president@whitehouse.gov", we can't just block the whole whitehouse.gov domain. We can only block or rate limit the IP address.

But In Email 2.0, only mails from "Verified Strangers" will be accepted. That means, mail is REALLY coming from the said domain since the domain is either whitelisted the IP address or mail received from one of their MX servers. So, stranger reputation not only tied to the IP address, but also tied to the domain.

So if you send spam mails via our "Injection Phase", you are converting yourself from "Verified Stranger" to "Verified Spammer". In such cases, we not only block your domain and IP address, but also build a block list similar to Spamhaus Block List (SBL)[76] and then publish your domain and IP address there to help others.

Forwarded Mails

It's much easier to classify the sender as either "Verified Stranger" or "Unverified Stranger" when the mail is hosted on our server. If the sender is an "Unverified Stranger" then we can reject the mail immediately.

But it's getting complicated when the mail is hosted on third party servers. e.g. gmail.com. We don't have control over Gmail servers. So we can't reject the mail.

When a mail is hosted on third party servers, we will provide a unique mail forwarding address.

Email address structure:

> Domkey+LocalPart=HostPart@ReceiverDomain

e.g. If we create a box for third party mail account "johndoe@gmail.com" the mail forwarding address would be "giri123+johndoe=gmail.com@domboxmail.com"

[76] https://www.spamhaus.org/sbl/

Note: Domkey may be renamed to “BoxKey” in the future since it is being used for both Domboxes as well as Mailboxes.

Also Note, We extract the domain found in between = and @ symbol (gmail.com in this case), Fetch SPF record of that domain to make sure that the sending IP address is authorized to forward mails to that box. Only gmail.com SPF record IP addresses authorized to forward mails to the box giri123+johndoe=gmail.com@domboxmail.com.

When a forwarded mail get received in our server, the “Sending IP aka. Client IP” will be the Forwarding Server IP address (e.g. Gmail). Not the original Sender IP address.

But the good news is that Gmail, Outlook and YahooMail adds the “Received-SPF” header. So we are gonna rely on those information to extract the original sender IP address.

Gmail

```
Received-SPF: pass (google.com: domain of giri@dombox.org designates 209.85.220.41 as permitted sender) client-
ip=209.85.220.41;
```

Figure 130: Gmail Received-SPF Header

Outlook

```
Received-SPF: Pass (protection.outlook.com: domain of dombox.org designates
209.85.214.46 as permitted sender) receiver=protection.outlook.com;
```

Figure 131: Outlook Received-SPF header

YahooMail

```
Received-SPF: pass (domain of dombox.org designates 209.85.214.45 as permitted sender)
```

Figure 132: Yahoo Received-SPF Header

The Received-SPF header would be one of these[77] values.

We are gonna perform our “Authorization Layer” check based on the information found in the “Received-SPF” header.

When the mail get forwarded, our system gonna work exactly like it works for our hosted mail accounts, but when the sender is “Unverified Stranger” , then the mail will be moved to “Trash” folder instantly. It will be kept there for 30 days and then it will be deleted automatically.

Reputation

Gmail, Outlook and YahooMail are reputed mail services. We can trust them. But we cannot trust every forwarding servers.

A forwarding server can lie by forging the Received-SPF header info.

For example, you buy a domain called “xyz.com”, setup mail forwarding in your server, forge “Received-SPF” header and then forward the mail to our server. We cannot send challenge mails since we cannot trust xyz.com “Received-SPF” header. Our domain reputation will be at risk when we send challenge mails to wrong people. {Refer backscatter attacks}

So when the forwarding server is not in our “Trusted List”, we will send the Challenge mail via the POP or IMAP instead of using our domain. i.e. Envelope From and Message From for the challenge mails will be ending with @xyz.com instead of @domboxmail.com when viewed by the receiver.

Private Mailing System

All of those “Injection” phase methods like CAPTCHA, Phone Number, PoW etc. are Optional. You can be disable those methods.

In fact, you can disable the whole “Injection” phase itself. In such case, the system will be treated as “Private Mailing System”

[77] http://www.openspf.org/SPF_Received_Header

Via “Isolation” you allow only certain “Websites” to mail you and via “Restriction” you allow only certain “Individuals” to mail you. Since there is no “Injection” phase, mail from the “Strangers” will be rejected.

By default, Injection phase will be active when you enable Restricted Mode. When a mail is coming from a “Unverified Stranger”, the mail will be rejected with the following error message.

550 Restricted Box. Unauthorized and Unverified Sender. Please configure SPF or Send this mail from one of your MX server IP address

But if Injection phase is disabled, mail will be rejected from all type of “Strangers”. i.e. No mail will be accepted from “Strangers”.

Even the mails from “Verified Strangers” will be rejected with the following error message.

550 Restricted Box. Unauthorized Sender.

Let’s go over the Sample SMTP chat one more time.

> mail.example.com Connecting to mail.domboxmail.com with its IP address
>
> domboxmail.com => 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> example.com => HELO mail.example.com
>
> domboxmail.com => 250 Hello, nice to meet you, mail.example.com
>
> example.com => MAIL FROM: <john@example.com>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <user1@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => RCPT TO: <user2@domboxmail.com>
>
> domboxmail.com => **550 Restricted Box. Unauthorized Sender.**
>
> example.com => RCPT TO: <user3@domboxmail.com>
>
> domboxmail.com => 250 OK

> example.com => RCPT TO: <user4@domboxmail.com>
>
> domboxmail.com => **550 Restricted Box. Unauthorized Sender.**
>
> example.com => RCPT TO: <user5@domboxmail.com>
>
> domboxmail.com => 250 OK
>
> example.com => DATA
>
> domboxmail.com => 354 End data with <CRLF>.<CRLF>
>
> {Message Part goes here}
>
> domboxmail.com => 250 OK, message accepted for delivery: queued as 12345
>
> example.com => QUIT
>
> domboxmail.com => 221 Bye

As you can see, the contact john@example.com not found in user2 and user4 Address Book. So we rejected the mail for those recipients instantly and selectively.

The mail will be accepted for the other 3 users.

In Private Mailing System, the receiver needs to whitelist the contact either manually adding it in the Address Book or Sending a mail to that contact. i.e. All outgoing mail contacts will be automatically whitelisted.

When both sender and receiver use their mail system as Private Mailing System, then contacts need to be whitelisted in both sides.

Phishing Prevention

Phishing is not possible in both “Isolation” and “Restriction”.

In Isolation, If you signup to “facebookmail.com” using a Dombox mail address, the box won’t accept any emails from facebook**e**mail.com unless it got whitelisted via SAD. So you cannot be deceived.

In Restriction, you are gonna add only the people you know in the “Address Book”

So Phishing can only be possible via “Injection” phase. Because that phase, accepts mail from strangers.

Whenever a stranger mail get injected via “Injection” phase, the mail would look like this.

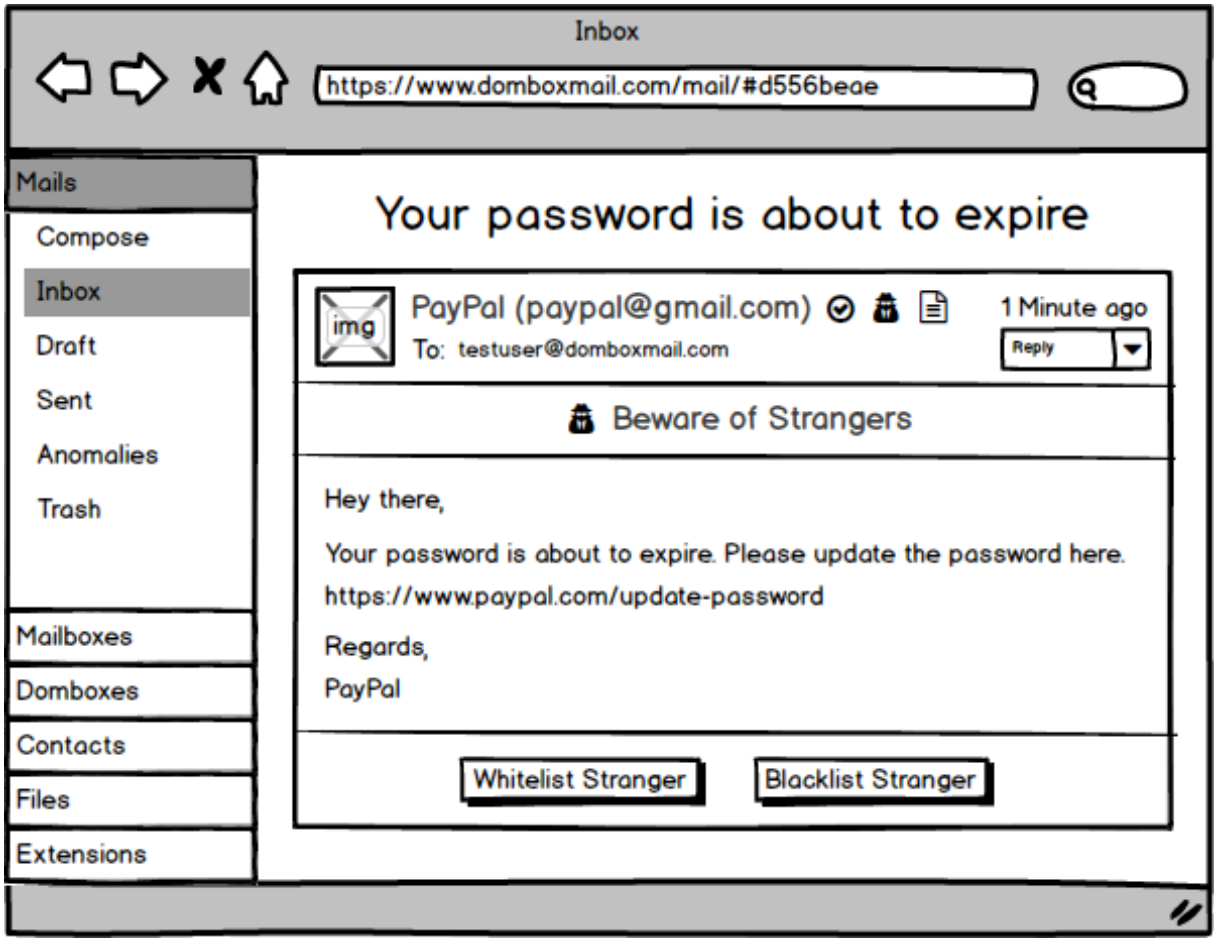


Figure 133: Injected Mail

The above mail hyperlinks to an incorrect URL.

Whitelist Stranger - Adds the sender to the whitelisted contacts in the “Address Book”. Note: If you reply to the mail, the sender will be automatically whitelisted. This is because no one would respond to the spammer mails.

Blacklist Stranger - Adds the sender to the blacklisted contacts in the “Address Book”

Ignore Stranger - If you don’t take any action, then the Stranger need to go through the “Injection” phase again next time.

The “Beware of Strangers” nag always appear in the Injected mails. If the user click the “Beware of Strangers” link, the warning message would look like this.

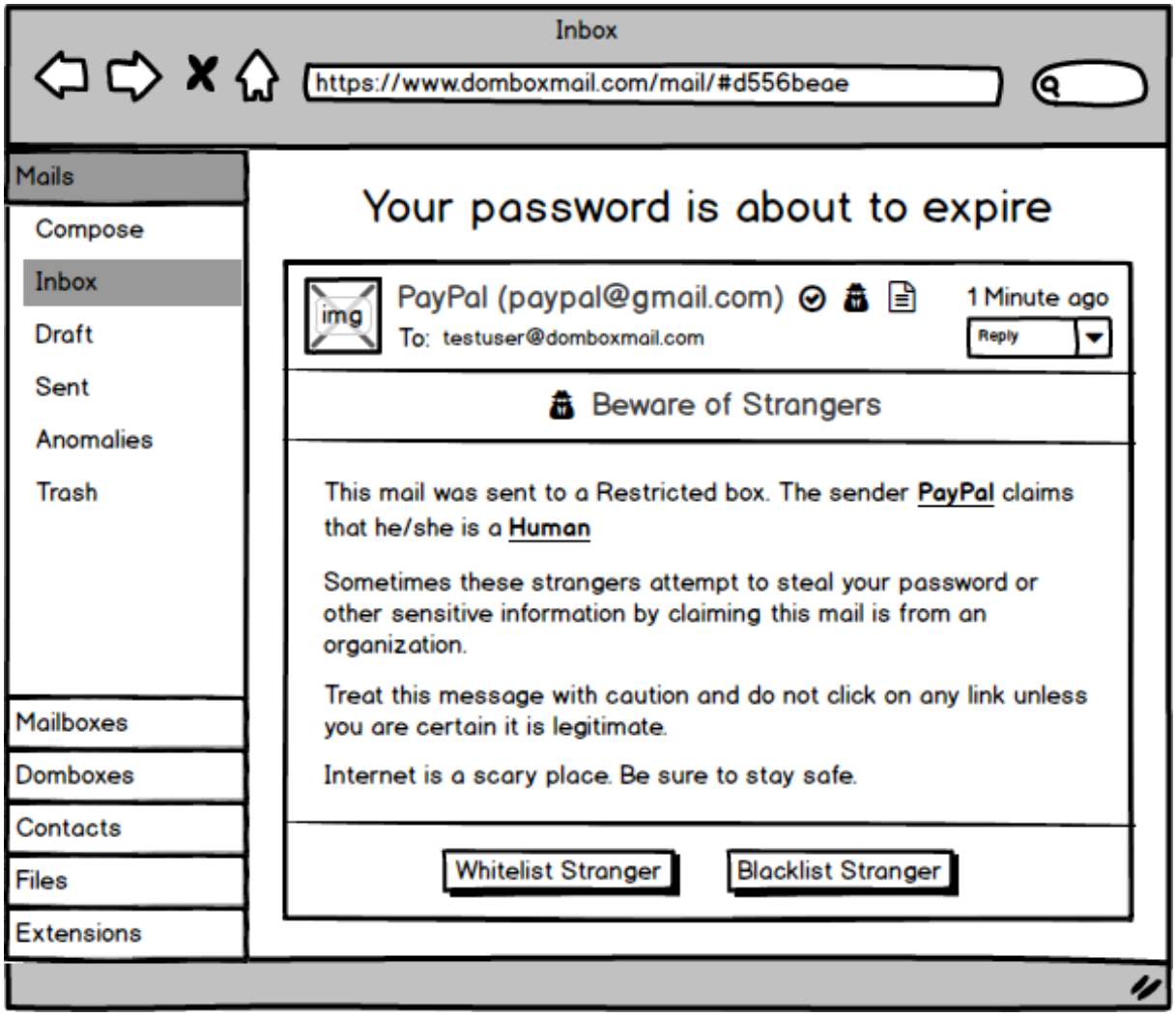


Figure 134: Beware of Strangers

“Injection Receipt” can be viewed in the Stranger mails by clicking the “Receipt” icon.

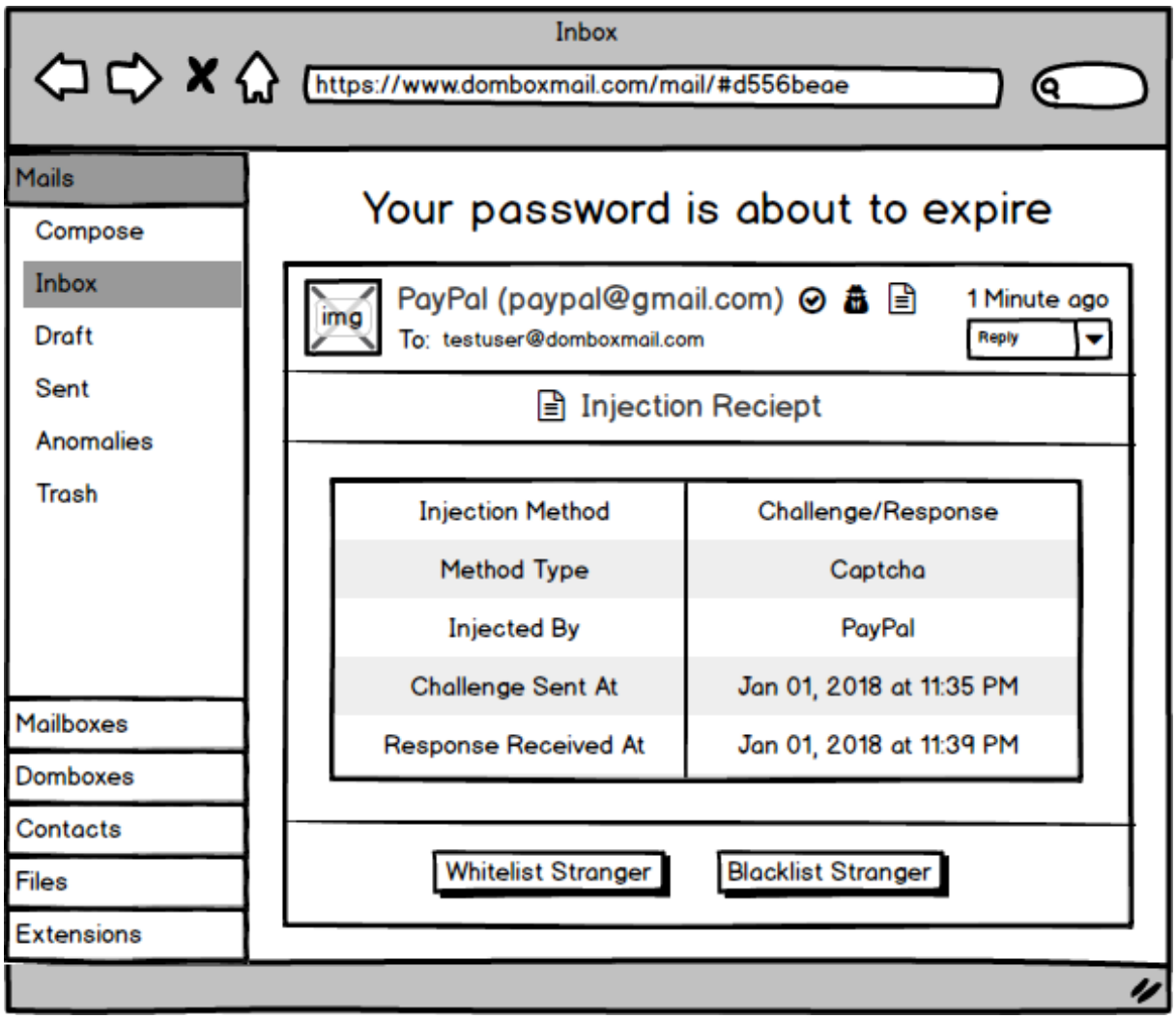


Figure 135: Injection Receipt

Thus, our system can solve the “Phishing” problem. Sweet…

Questions

Do you really think people would pay money to send mail?

First of all, Attention Fee in one of the injection methods. So it's a choice. Not the complete solution.

An average Internet user does not go for Attention Fee, but a busy CEO would go for that.

No one can question you if you put your mobile in silent mode. It's your mobile. You can do whatever you want.

So at the end of the day, it's all about the receiver's preference. If the receiver says you need to pay the fee to mail them, then you can either pay the fee or just walk away.

The "Attention Fee" is applicable only for "Strangers". And the receiver is gonna return that money anyway.

So from the recipient perspective, a better question you have to ask yourself is that "Is it really worth spending your time with someone who can't afford the fee you set?"

If the answer is "Yes", then disable the "Attention Fee" and stick with other methods like "CAPTCHA", "Phone Number" etc.

Who gets the Attention Fee money, when the receiver mark my mail as Spam?

If the receiver doesn't respond to your mail or mark you as a spammer, then the money will go to our system. The purpose is not to make money here, but to encourage refunds.

If we reward that money to the receiver, then that would become a money-making scheme. Some people would mark the sender as a spammer even if they know that person to make money. But if the money goes to our system, most likely they would refund the money.

If the refund is not initiated within 30 days, then our system takes the money, not the receiver.

Keep in mind, no spammer would pay the Attention Fee just to mail you unless this spammer is REALLY a nigerian prince. If someone make the payment, then 99% of the time, it's a genuine person. So you are encouraged to refund the money instead of putting in your pocket.

Would this solution work for all email users on the Internet?

Yes, As long as your senders are ok with filling CAPTCHA.

Isn't challenge/response mechanism used by Isolation phase already patented by other companies?

Yes

Patent name => Method and system for filtering electronic messages[78]

Originally invented by Christopher Alan Cobb in 1997, but currently assigned to Google.

However, that patent got expired recently. So we are legally allowed to use C/R mechanism in the Injection phase.

Chapter 17: Site Classifications

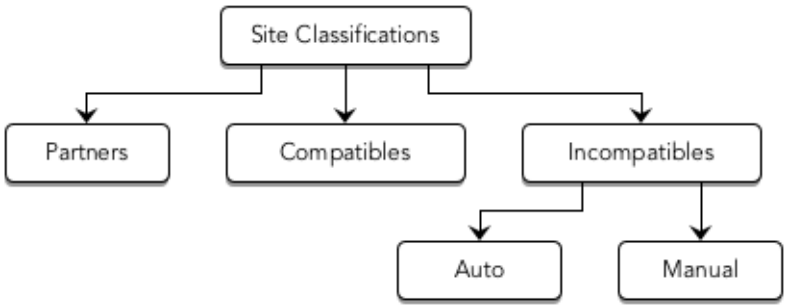


Figure 136: Site Classifications

Websites are classified into three major categories. Partners, Compatibles and Incompatibles.

[78] https://patents.google.com/patent/US6199102B1/en

Incompatible Sites are further classified into two categories. Auto Incompatibles and Manual Incompatibles.

Partners (aka. Portal Partners) are the sites that display our "Teleport" button.

Compatibles are the sites that accept the Dombox mail address. 99.99% of the domains in the world are compatible with Dombox mail address.

Incompatibles are the sites that are unable to accept the Dombox mail address.

Auto Incompatibles are the sites that are unable to accept the Dombox mail address because the dombox email address local part exceeds 64 characters. i.e. Not compatible with the email standards

Manual Incompatibles are the sites that block the Dombox mail addresses intentionally by hardcoding it. e.g. A site that sells your data won't be interested in Dombox addresses. So they usually force the users to provide other email address.

In Domboxes when a domain is a "Partner", a green check icon will be displayed right next to the domain. When a site is "Incompatible" a red "x" icon will be displayed right next to the domain.

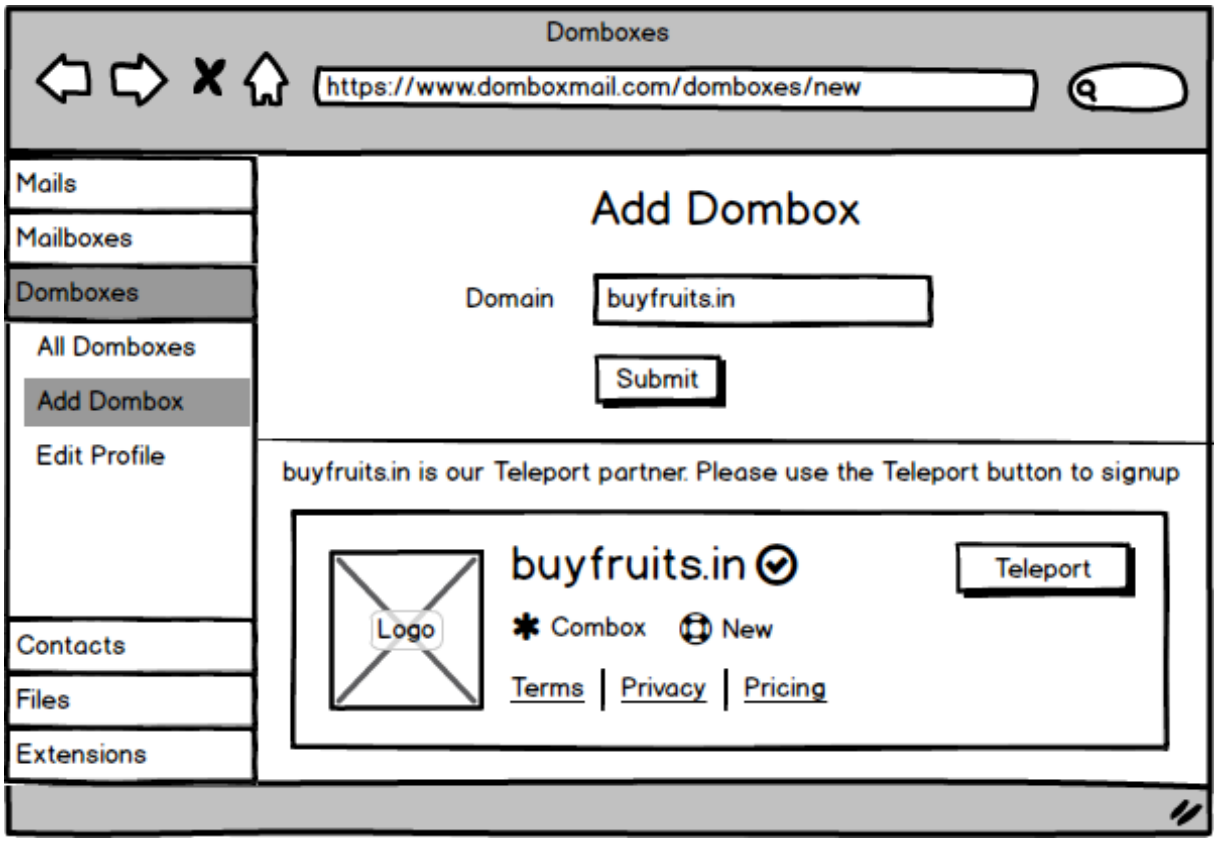


Figure 137: Partner Notice

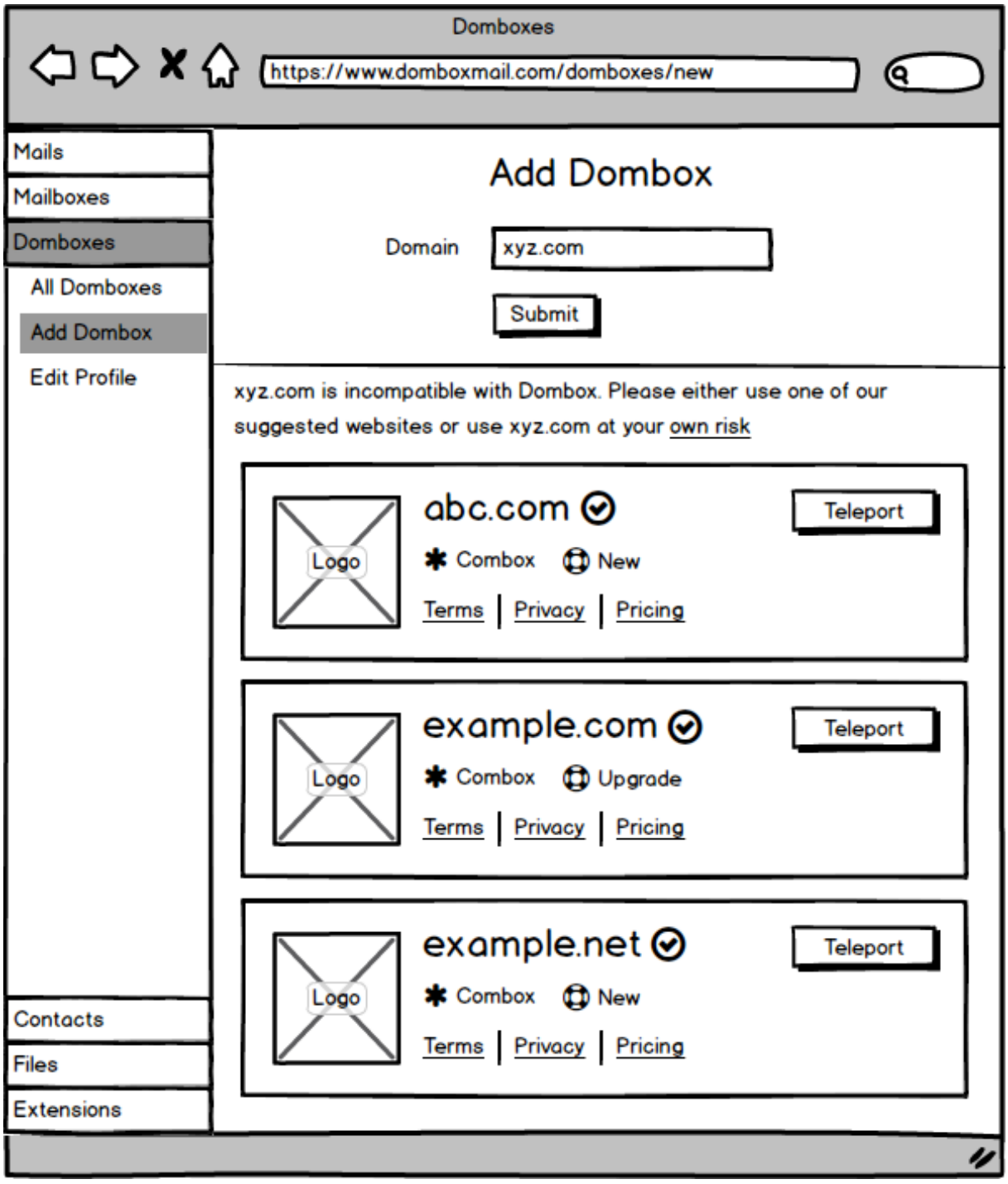


Figure 138: Incompatible Warning

Rogue Sites

Some rogue websites, usually make a living by selling your data

They are not gonna be happy with “Dombox mail addresses”. Because “Dombox mail address” pose a different threat to them. i.e. “They can’t sell your data anymore”

Only the Dombox Domain and its SAD domains can mail you.

If they allow a data buyer’s domain via SAD, then they will be caught red-handed.

So they would go for one of the following two things

Block Dombox email addresses. i.e. Manual Incompatible. When they choose this option, they are creating a problem what we call “Hogwarts Problem”

Their second option would be forcibly asking your primary box address since Primary box can accept mail from anyone. When they choose this option, they are creating another problem what we call “Hourglass Problem”

Hogwarts Problem

Figure 139: Hogwarts Problem

Hogwarts is a Wizardry school in the Harry Potter series. In the first part, Harry Potter receives the "Acceptance Letter" mail from "Hogwarts" via owl post. Due to "Man-In-The-Middle" attacks, delivery get failed and then Hagrid later deliver the mail to Harry Potter in person.

Now here comes our question. What would have happened if Harry Potter never received the mail OR received the mail but read it after 6 months?

Most likely he would have joined some other school instead of Hogwarts. Right?

Same here. When a website becomes an "Incompatible" website, that means they are forcing their users to provide some other mail service address.

Dombox is the only working zero spam mail solution out there. When Dombox mail service gains popularity, the users are going to use their old mail service very less. Because we solved a bigger pain point. Well... actually more than a dozen pain points. Since our product doesn't rely on user engagement problem like you see in a social network, it's a scalable business. Put it this way, if our solution works for 1 person, then it's gonna work for 1 billion users too.

You can ignore us on Day 1. But you can't on Day 1000. Because by then, we would have made a noticeable difference to the world. Tell us this... How many times do you check your old Myspace or Orkut account or your old mail account?

If Facebook suddenly stops sending notification emails for 1 month, it will reflect in their quarterly earnings. Because those notification emails are the ones that bring back users to their platform.

When you force your users to use other mail services, you are delaying the user's attention.

If you are still not convinced, Let us give you more thoughts on this.

The internet currently has 332 million domains. That doesn't mean 332 million unique business available on the internet. If you count the unique businesses in the world, it would be far less than 100,000. So we are all competing to get a piece of the market.

Out product may look like something new to the market. But, at the end of the day, its just another mail service that's competing with Companies like Google and Microsoft

So.. Customer acquisition is a time-sensitive thing. If you don't convert your customer on time, most likely some other business will.

Also note, If you become an incompatible website, you are creating a "Moral Dilemma". So make sure to have a valid reason for your users. By default, your website is a compatible one since our i-mail address is fully compatible with SMTP. That means users can manually create a Dombox and then signup to your website. Since there is no Contract, a user can delete the box anytime he/she wants. So that's a big advantage for users and big disadvantage for your business. When your site is a compatible one, you are neither supporting us nor opposing us.

Email spam is most likely a bigger issue than whatever reason you have in your pocket. So we don't think you can justify that.

Being an "Incompatible" website explicitly says that you are selfish and you don't care about your users. You are obstructing a lot of things. Their right to spam free life, Their right to privacy etc. So It's gonna put your business in a bad light.

If you become an "Incompatible" website, then we believe, you may have issues with these two things.

1. Teleport button
2. 5 layers passed emails.

Without the Teleport button, it's hard to establish a contract. Without a contract, we cannot revoke the offline and delete privileges from the user. So that explains it.

As for "5 layers passed emails" if we accept emails even when layers are failed, then the box is vulnerable to email forgery. A user can send a spoofed spam mail to themselves, but blame it on you by saying you are breaching the terms.

So the "5 layers passed emails" not only protect the users from receiving spam, but also protect your business from breaching the terms.

Keep in mind, we are fighting for a good cause. So its much easier to convince the world. If you take the "Incompatible" route, sooner or later you are gonna kill your business if we become successful.

Hourglass Problem

Figure 140: Hourglass Problem

When a website forcibly ask the user to provide their Primary (P) box address, they are creating the “Hourglass Problem”. Some websites would do that to collect email address and sell it to third parties.

Websites should also take the “Restricted Mode” into account when forcibly asking for user’s “Primary” box address

Boxes found under Domboxes group give the websites exclusive unrestricted access to their box, whereas the primary box is not.

For “Restricted Mode”, we are planning to bring a “Scan for new Contacts” feature. Every time you turn on the “Restricted Mode”, a scan will be initiated since the time you turned off “Restricted Mode” mode. The new contacts found during the scan will be marked as “Recognized” contacts upon user confirmation.

e.g. A user signed up for example.com with his Primary (P) box address. The website sends the welcome email from “no-reply@example.com”. A week later the user decided

to use the “Restricted Mode” option. This time, we will be scanning for the new contacts during the time “Restricted Mode” turned off. Now, example.com is completely locked out from Primary (P) box except this one contact. no-reply@example.com This is what we call “Hourglass Problem”.

i.e. The path is very narrow here just like you see in the hourglass. Only the early contacts who mailed the user before activating the “Restricted Mode” can able to mail the user in the future.

Chapter 18: Miscellaneous

Anomalies

What is spam? In simple terms, it’s the emails that are sent by a spammer. Right? This spammer is most likely someone you are not familiar with.

Now think about from the “Isolated Mailboxes” perspective. Those boxes are created with your knowledge. So you know exactly what you are signing up for.

You know the website. Mail passes all 5 layers. Everything seems fine. But just because a mail passes all those 5 layers, doesn’t mean it’s always going to be a genuine mail.

There are legitimate reasons for a mail not to be genuine. For example, you signed up for a website. However, that website got hacked at some point. The hacker uses the website servers to send out emails.

In such situations, you are not the only victim here. The website too. If the website recovers from the hacker, then everything’s goes back to normal. Because your email address is valuable only when the hacker can use the original website servers. If the hacker uses some other servers to send out emails, then some layers gonna fail due to the DNS settings.

So we cannot blindly trust the mail even if they are our “Portal Partners”. After passing the 5 layers, emails coming to Domboxes will be passed again to a filter called “Anomalies Filter”. (Note: Mailboxes mails will be passed to “Anomalies Filter” only when Restricted Mode active)

Anomalies filter would scan all the links found in the mail and make sure they are ok. For example, a link that linking to some unknown third party website would seem more fishy, than the link that links to the Dombox domain or the domains found in the SAD record.

If the emails are caught by Anomalies Filter, then the emails will be put in Anomalies folder. Keep in mind, emails found in Anomalies folder might be more dangerous than your typical spam mail.

If you are a website owner, link to third party websites only when it's absolutely necessary. Of course, you are welcome to link to popular websites like Facebook, Twitter, Youtube etc.

Anomalies Filter and Anomalies Folder applicable for all boxes found under Domboxes. And "Restricted" Mailboxes.

Here is the definition of Anomaly from "Oxford dictionary" if you are hearing the term for the first time.

"Something that deviates from what is standard, normal, or expected"

Mailing List / Discussion List

> A **mailing list** is a collection of names and addresses used by an individual or an organization to send material to multiple recipients. The term is often extended to include the people subscribed to such a list, so the group of subscribers is referred to as "the mailing list", or simply "the list".

A mailing list is usually created for sharing views on specific topics. e.g. Computers, Politics etc.

Let's understand how mailing list works.

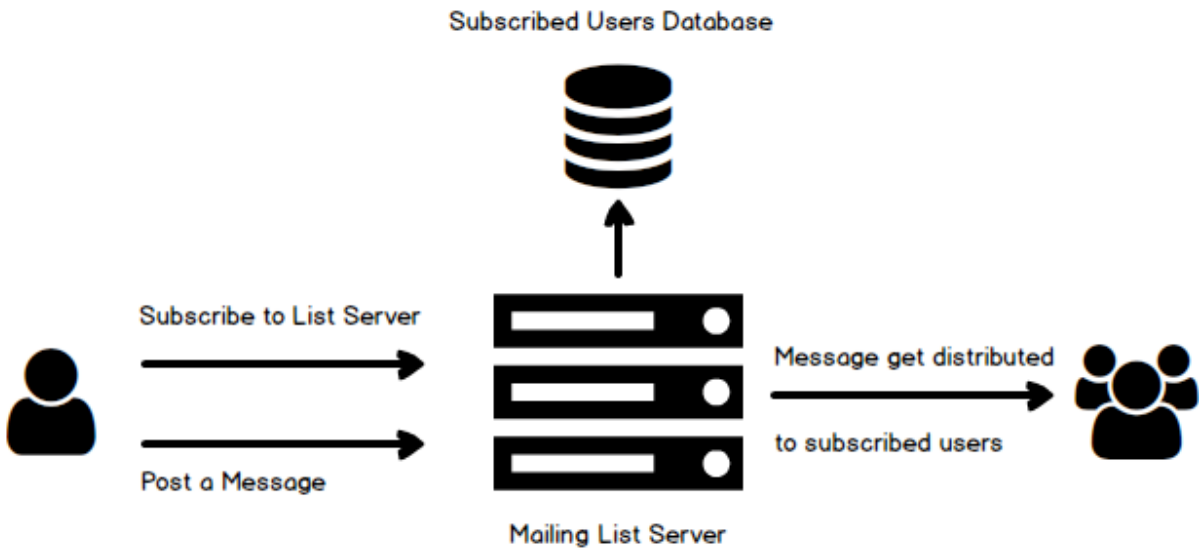


Figure 141: How Mailing List Works

In a mailing list, there are usually thousands of subscribers like you. There will be an address for posting the message.

Let's say, politics@listserver.com is the mailing list post address. When you post a message, listserver.com forwards the message to all the subscribers.

For example, when the user Giri post a message, the message would look like this when viewed by others.

> Envelope From: politics@listserver.com
>
> Message From: giri@dombox.org

The point here is that the "Message From" domain can be any of those 332 million domains. But "Envelope From" domain is gonna be listserver.com

listserver.com is the mediator here. So, create an "Isolated Mailbox" for listserver.com.

e.g. test123$listserver.com@domboxmail.com

Use that address when posting a message to listserver.com

There is one problem while receiving mails.

Our Alias Layer has two sub-layers. Envelope Layer and Message Layer. Both Layer needs to be passed to accept mails.

However, we need to have an exception for the mailing list. We should accept mails even when the “Message Layer” result is Fail.

There are two ways we can achieve that.

Option 1:

We should let the users mark the box as “Mailing List” box. We should provide an option like “Mark as Listbox”. When a box is marked as “Listbox”, we are gonna accept mails even when the “Message Domain” related check result in “Fail”. Applicable only for Domboxes {Dombox, Hybrid and Combox}

Option 2:

Let the “Dombox Domain” explicitly states that the domain is a Mailing List domain.

So we should have an option in the SAD record to mark the domain as a mailing list domain.

> e.g. _sad.listserver.com => “v=sad1 list:yes -all”

The above sad record says, treat the current domain as a “Mailing List” domain.

If only one subdomain used, then the domain can explicitly state that like this.

> e.g. _sad.listserver.com => “v=sad1 list:discussion.listserver.com -all”

The above sad record says, treat only the “discussion.listserver.com” as a “Mailing List” domain. For all others, regular SAD rules apply.

If more than one subdomain used, then the domain can explicitly state that by separating with comma.

> e.g. _sad.listserver.com => “v=sad1 list:politics.listserver.com,movies.listserver.com -all”

In the last example, listserver.com asks us to treat only the following subdomains as “Mailing List” domains. politics.listserver.com and movies.listserver.com. For all others, regular SAD rules apply.

Note: In mailing lists, Message SAD and DMARC always gonna fail. So we have to rely on SPF for detecting forged mails.

STRIPTLS Attacks

SMTP encryption is an Opportunistic Encryption. A man-in-the-middle attack can be initiated in the Opportunistic TLS that's known as "STRIPTLS" attack.

In STRIPTLS attack, the attacker gonna strip the STARTTLS command. An experienced attacker may make the command unrecognized by replacing the characters to make it compatible with the Packet Size. e.g. STARTTLS => STARTXXX

Here is an Example

> mail.example.com connecting to mail.yahoo.com with its IP address
>
> 220 mail.yahoo.com Yahoo ESMTP Service Ready
>
> EHLO mail.example.com
>
> 250-Hello, nice to meet you, mail.example.com
>
> 250-SIZE 1000000
>
> 250-8BITMIME
>
> 250 STARTXXX

In then last example, the client (sender) is asking "Hello, What are the extensions do you support?" and the receiver (server) responds with the list of extensions.

The attacker replaced the STARTTLS command in the last example. Since the client (sender) doesn't recognize the STARTXXX command, the whole mail will be transferred in "Plain Text". Some ISPs[79] in the US and Thailand performed this attack on their customers back in 2014.

STRIPTLS attack is a serious issue. An attacker can hijack your social media account with the help of STRIPTLS attacks.

[79] https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks

e.g. Attacker Initiate forgot password request in Facebook, perform STRIPTLS attack. Now the attacker has your password reset confirmation link. We are using Facebook as an example. It can be applicable for any sites that let's you reset your password with a confirmation link.

We can fix that problem in Domboxes.

If the following record found in the Dombox Domain, then all the mails coming to that Dombox must use the Encryption. Or the mail will be rejected.

> e.g. _sad.example.com => "v=sad1 tls:yes -all"

Implicit VRFY

VRFY is one of the SMTP commands introduced in RFC 821[80]. VRFY command asks the server to verify an address.

Most mail servers do not support VRFY command in order to prevent abuse. For example, spammers can use the VRFY command and scrap valid email addresses and send spam mails later.

Although we don't advertise VRFY command in our supported SMTP commands list, we implicitly support VRFY command only for i-mail addresses when the following conditions are met.

1. The MAIL FROM domain must be the "Dombox Domain"
2. The CLIENT IP address must be whitelisted in the MAIL FROM domain i.e. Verified Envelope Domain
3. VRFY command must provide a valid i-mail address
4. i-mail address Dombox Domain must match the MAIL FROM domain

Example:

A user created a Dombox for quora.com

Quora.com can verify whether the Dombox exists or not without sending a verification mail to the user.

[80] https://tools.ietf.org/html/rfc821

> mail.quora.com Connecting to mail.domboxmail.com with its IP address
>
> 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> HELO mail.quora.com
>
> 250 Hello, nice to meet you, mail.quora.com
>
> MAIL FROM: <noreply@quora.com>
>
> 250 OK
>
> VRFY: <test123$quora.com@domboxmail.com>
>
> 250 OK
>
> VRFY: <hello123$twitter.com@domboxmail.com>
>
> 550 Unauthorized verification request. Decline to answer
>
> QUIT
>
> 221 Bye

Better Performance

Our system can offer better performance than traditional mail system.

The whole system is designed to reject mails selectively during the RCPT TO command in both Domboxes and Mailboxes. Thus, it can provide better performance.

> mail.example.com Connecting to mail.domboxmail.com with its IP address
>
> 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> HELO mail.example.com
>
> 250 Hello, nice to meet you, mail.example.com
>
> MAIL FROM: <john@example.com>
>
> 250 OK

> RCPT TO: <giri123$example.com@domboxmail.com>
>
> 250 OK
>
> DATA
>
> 354 End data with <CRLF>.<CRLF>
>
> From: John Doe <john@example.com>
>
> To: Giri <giri123$example.com@domboxmail.com>
>
> Date: Fri, 01 January 2015 16:02:43 -0500
>
> DKIM-Signature: s=selector123; d=example.com; .....
>
> Subject: Thanks for Signing Up
>
> Thanks for signing up for Example.com.
>
> Click <this link> to get started.
>
> Regards,
>
> John Doe
>
> .
>
> 250 OK, message accepted for delivery: queued as 12345
>
> QUIT
>
> 221 Bye

You see the DATA command?

A mail system that relies on spam filters need everything found after the DATA command. But our system is designed to deal with the spam mails before the DATA command.

An incoming mail can be upto 25 MB in most mail servers. Go figure the amount of bandwidth get wasted in dealing with 60 Trillion spam mails.

There are few other issues too. Wasting time and computing power in spam and virus checks. Sending bounce mails etc.

If we can reject the mail before the DATA command, then the bandwidth wastage will be so

tiny while compared to the traditional email system. 1KB can hold 1024 ASCII characters. So the bandwidth wastage will be in bytes rather than MegaBytes.

This is how we deal with mails coming to Domboxes.

> mail.example.com Connecting to mail.domboxmail.com with its IP address
>
> 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> HELO mail.example.com
>
> 250 Hello, nice to meet you, mail.example.com
>
> MAIL FROM: <spammer@example.com>
>
> 250 OK
>
> RCPT TO: <giri123$twitter.com@domboxmail.com>
>
> 550 Alias Layer Failure

So the mail got rejected before the DATA command.

As for Mailboxes, when a mailbox is in “Restricted Mode” that says, it can accept only “Conversational Mails”

So when looking for Authorized Personnel in the address book, we are looking whether the MAIL FROM address is whitelisted or not. [Restriction Phase]

And the challenge mails will actually be sent to the same MAIL FROM address. [Injection Phase - Verified Stranger]

If the MAIL FROM address is not a “Verified Stranger”, then the mail will get rejected before the DATA command itself. [Injection Phase - Unverified Stranger]

> mail.example.com Connecting to mail.domboxmail.com with its IP address
>
> 220 mail.domboxmail.com Dombox SMTP Service Ready
>
> HELO mail.example.com
>
> 250 Hello, nice to meet you, mail.example.com
>
> MAIL FROM: <spammer@example.com>

> 250 OK
>
> RCPT TO: <testuser@domboxmail.com>
>
> 550 Restricted Box. Unauthorized and Unverified Sender. Please configure SPF or Send this mail from one of your MX server IP address

So spam mails to both Domboxes and Mailboxes actually gets rejected before the DATA command itself.

If an average mail size is 100KB, that means our system is 100x more efficient than Email 1.0

i.e. No bandwidth wastage, No storage wastage, No spam checks, No virus checks, No bounce mails, No False Positives, No False Negatives, No Backscatter Attacks, No Backscatter Relay, No Botnet Spam

Isolation Tools

Our product's strength lies on the Isolation phase.

If our solution is hard to adopt, then it will result in failure even if our system solves the spam problem. So, we need to make this process easier for consumers as much as we can.

Let's say you are a gmail user who already have accounts in hundreds of domains. You would like to migrate to our system.

This is how your email addresses would look like in our system.

Isolation Phase: @domboxmail.com

Restriction and Injection Phase: @gmail.com

It's a very tedious job for the users to manually update their old email address with the new i-mail address in those websites. To make this process easier, we will provide automation tools.

iMacros is one of the well known browser automation tool. Here is a sample video[81] that automates flight search.

[81] https://www.youtube.com/watch?v=t2Mi8bVRlX4

We will build such browser extensions only for the “Dombox Isolation” job. We will collect the automation formula from the first few users and automate it for the rest of the users. The users only have to intervene in cases like captcha filling, Teleport consent screen etc.

When users import their old mails, we will analyse it and provide the results. We actually scan for the “Message Domain” in all your mails and sort the unique domains by alexa rankings. Higher alexa rank means important domain.

This is also your chance to start over. Delete the domains you don’t need and keep only the domains you consider as important.

Here is a screenshot from our prototype where the Gmail mails are analyzed.

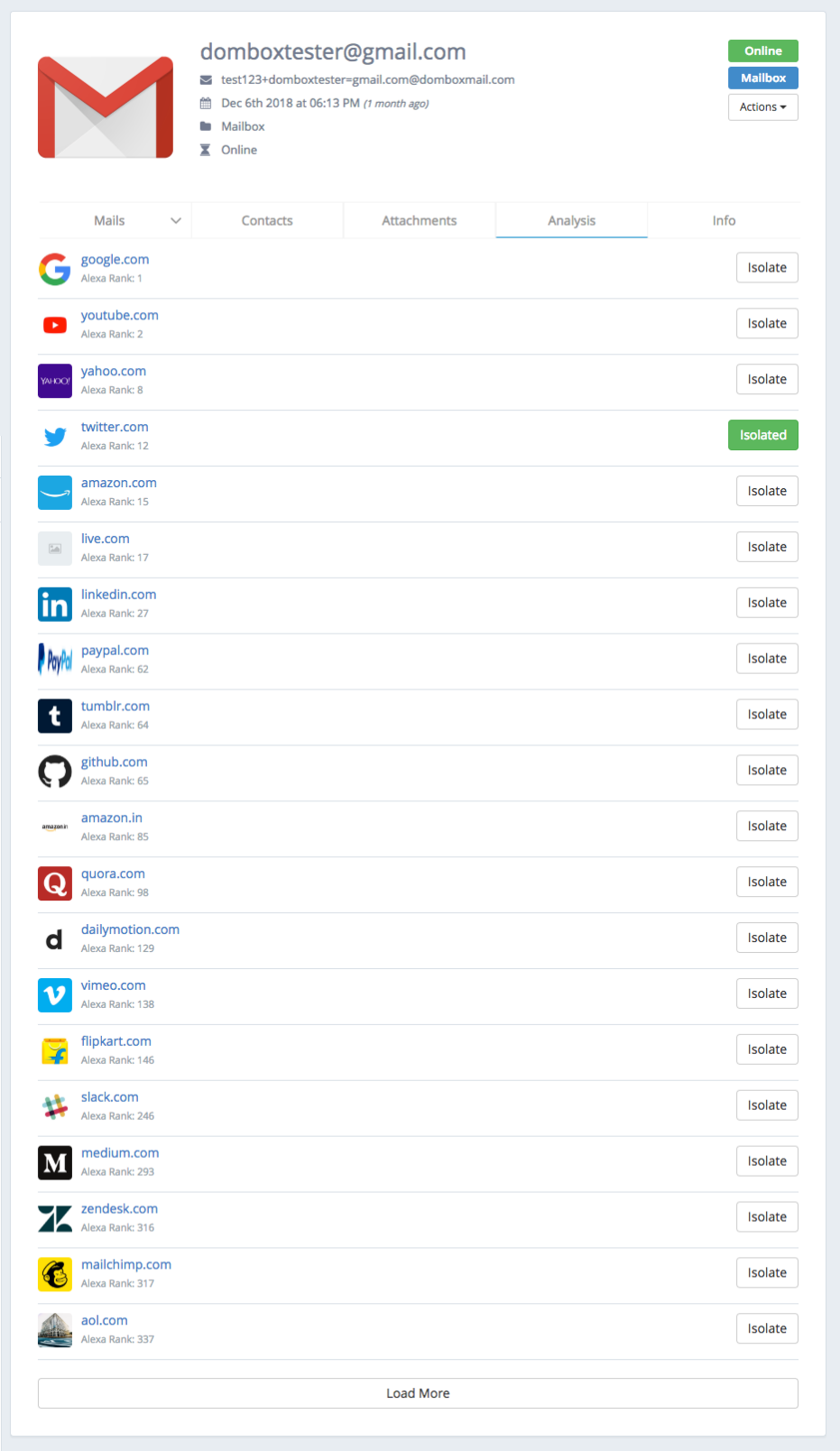


Figure 142: alexa

Our mail system is not compatible with the traditional mail clients. So we have to build our own mail clients.

Today we have projects like Chromium Embedded Framework (CEF)[82] for embedding browser within another application. We probably use such framework in our mail client. In such case, if you click the "Isolate" button you see in the last screenshot, a browser popup would appear and automate most of the process.

Ever heard of password managers like 1Password[83], Dashlane[84], LastPass[85] ? Most likely we will build similar tools for non portal partner domains.

Password managers are taking care of the "password" field. We are gonna take care of the "email" field.

Note: We will be primarily focusing on the automation formula for the alexa top 1 million domains.

Box Comparison

	Primary (P)	Mailbox (M)	Dombox (D)	Hybrid (H)	Combox (C)
Must Pass Layers	None	None	Alias	All	All
Max. Boxes	1	Unlimited	Unlimited	Unlimited	Unlimited
Price	Free	Paid	Free	Free	Free
Offline	No	Yes	Yes	Yes	No
Delete	No	Yes	Yes	Yes	No
Format	No	No	Yes	Yes	Yes
Mute	No	Yes	Yes	Yes	Yes

[82] https://en.wikipedia.org/wiki/Chromium_Embedded_Framework
[83] https://1password.com/
[84] https://www.dashlane.com/
[85] https://www.lastpass.com/

	Primary (P)	Mailbox (M)	Dombox (D)	Hybrid (H)	Combox (C)
Subscribe / Unsubscribe	No	No	Yes	Yes	Yes
Spam Folder	Yes*	Yes*	No	No	No
Anomalies Folder	No*	No*	Yes	Yes	Yes
Restricted Mode	Yes	Yes	No	No	No
Greylisted Mode	No	No	Yes	Yes	Yes
Creation Source	Signup Form	New Mailbox	New Dombox	Telescribe	Teleport

* When “Restricted Mode” active, the value will be inverse.

Chapter 19: Internet Privacy

In our opinion, the current internet lacks privacy.

The word “Privacy” may sound like a “Rich” people problem, but the truth is “Normal” people don’t quite understand the importance of it.

Allow us to explain why current internet lacks privacy with an Example.

Gravatar

Have you ever heard of a site called Gravatar[86]? It is one of the most popular avatar services on the internet. Gravatar stands for “Globally Recognized Avatar”

Before the inception of Gravatar, you need to upload your avatar manually in every website you sign up. But after Gravatar, it’s all “one” avatar.

According to their stats, they are serving the avatars over 8.6 billion[87] times in a day.

[86] http://en.gravatar.com/
[87] http://en.gravatar.com/#user-logos-container

WordPress[88] is a popular open source software. More than 60 million[89] websites you see on the internet powered by that software. This software comes with Gravatar by default. So more than 60 million websites today supports Gravatar.

Even many of the major professional websites like StackOverflow[90], Github[91] etc depends on the Gravatar service for avatars.

This is how Gravatar works. You go to gravatar.com, signup with your email address and upload an avatar. This avatar is now linked to your email address.

Now, let's refresh our memories. What is a Hash?

Hash is a unique string that identifies the data, right?

Gravatar uses the **email hash** to build the avatar URL.

This is how your avatar image URL looks like. https://secure.gravatar.com/avatar/{MD5 email hash goes here}

Now if you signup to any third party websites or post a comment with your email address, then the Gravatar will be displayed if the site support it.

Although Gravatar solved a major issue, it created two more major issues.

Note: An average internet user may not notice these things. So we will try to explain clearly as much as we can.

Entropy

In a nutshell, Entropy[92] is the "Degree of Unpredictability"

You know what is the most common password on the internet?

Its "123456[93]"

[88] https://wordpress.org/
[89] https://www.forbes.com/sites/jjcolao/2012/09/05/the-internets-mother-tongue/
[90] https://stackoverflow.com/
[91] https://github.com/
[92] https://en.wikipedia.org/wiki/Entropy_(information_theory)
[93] https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Now... A hacker's first try would be trying that password. So entropy of that password is "literally zero". Because the hacker cracked the password in the first attempt.

To increase the Entropy, you need to pick a very strong password.

If we give you a "Hash" of an email address and ask you to find the real email address, you would be completely lost. Right?

e.g. 503A8F0B2D11DA49A27150C868A5EEB5 => ?????????@????????

Because there are Gazillion possibilities. The Entropy is very high. The value of this entropy depends on the possible email address combinations. So you have no idea where to start.

But if we give you the "Name" too, then it's going to make your job much easier. A man whose name "Donald Trump" definitely not gonna have an email address that looks like "barackobama@gmail.com"

Underline the word "definitely". Although you still have no idea about the real email address, you are "sure" of something now. So you weakened the entropy.

Let us give you the "Name" and "Email Hash".

Name	Email Hash
Jeff Bezos	503A8F0B2D11DA49A27150C868A5EEB5

Lets try the following combinations.

Email Address	Hash
jeff@amazon.com	27D637B6F491BCBEE2C87F13136B675E
bezos@amazon.com	12B79F144DBF4AA7FEADFD71679A2F91
jbezos@amazon.com	503A8F0B2D11DA49A27150C868A5EEB5

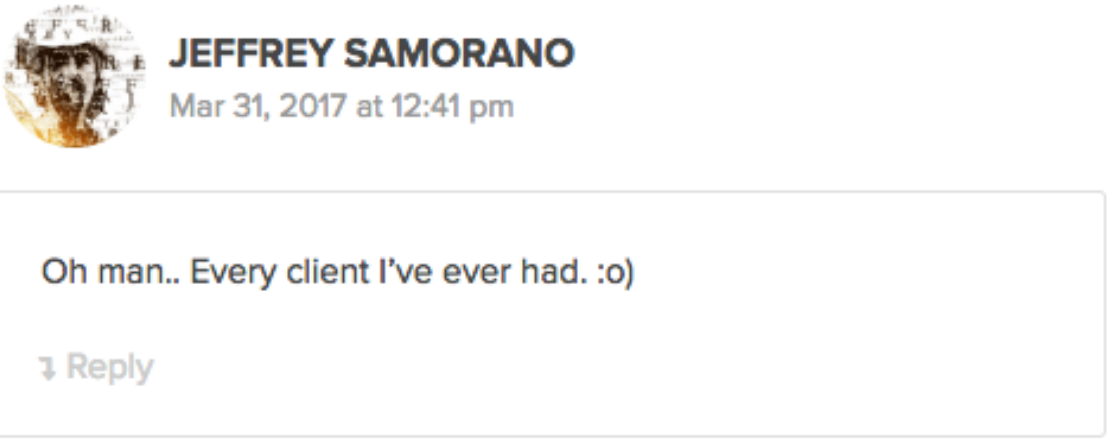
There.. we got the correct email hash in the last attempt.

So one thing is clear in the last experiment.

You can find “Valid Email Addresses” if we give you “Name” and “Email Hash”

But If we give you the “Date” too, then you can find the “Active Email Addresses” easily right?

For example, If a user post a comment within the past 6 months or 1 year, then most likely the user is an active email user



Email Hash + Name	Valid Email Addresses
Email Hash + Name + Date	Active Email Addresses

So Gravatar Major Issue 1: Email Brute-forcing

Issue 1: Email Brute-forcing

In the brute-force method, the spammers have to generate multiple email addresses and try sending an email to each generated email address. If the email got accepted then its a valid email address.

The success rate of this method will be very low. Let’s say the success rate is 5%, that means

95 out of 100 emails are failing. In such cases popular mail services like Gmail, Outlook etc. usually block and blacklist the spammer's IP address.

In Gravatar case, email brute-force / dictionary / combinations attacks are not going be an issue. All you have to do now is generate email hash based on the name you see right next to avatar and compare with the avatar email hash. If it matches then you found a valid email address.

A spammer can find a massive amount of Gravatar URLs by crawling the web.

Efficiency

Gravatar method is actually efficient too. Let's measure the efficiency

Total number of email users in the world: 3.8 Billion[94]

Although some users may have multiple accounts, let's go with one mail address for each user

So we have 3.8 billion email addresses

An average consumer computer can generate hashes in Millions per second

A high-end gaming computer that has a graphics card can generate hashes in Billions per second

Application-Specific Integrated Circuit (ASIC) is a chip designed for specific applications. For example, an ASIC designed for Bitcoin usually has a huge hash rate.

How much are we talking about?

Let us grab the screenshot for AntMiner S9[95]

[94] https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf

[95] https://shop.bitmain.com/promote/antminer_s9i_asic_bitcoin_miner/specification

Figure 143: AntMiner s9 Hash Rate

Can you tell us what "TH" stands for in that screenshot?

Exactly…

Trillion Hashes / Tera Hashes

In the screenshot they claim, the chip can generate up to 14 Trillion Hashes per second

If you try 1000 name combinations for each email address, you would use only 3.8 Trillion hashes for 3.8 Billion email addresses

So you have used roughly quarter of a 1 second to try all the email addresses available in the world

That's more efficient than sending emails to services like Gmail to validate email addresses. Wouldn't you agree?

Issue 2: Privacy

Gravatar means globally recognized avatar right? If you signup to any website that supports gravatar, then your avatar URL going to be the same and that is the problem here.

Let us explain clearly. Let's say you have a website example.com and you would like to support Gravatar.

There is no API for Gravatar. All you have to do is just take your user's email address and generate email hash

Now just load the following URL for the image. That's it.

https://secure.gravatar.com/avatar/{your user's MD5 email hash goes here}

If you can do that, then everyone in the world can do that too right? That is the problem here.

In Internet sex sells. There are plenty of people out there who use the same email address for everything from professional use to signing up for porn websites.

For the sake of our argument, imagine you are a girl who goes kinky in such websites and one of your colleagues is stalking you. Now if your colleague does a deep we scan, that would reveal all your activity if the site supports gravatar.

As far as we know Gravatar TOS doesn't exclude any such websites.

Even if the site doesn't support today, there is no guarantee it won't support in the future.

To be quite honest, we are less concerned about the porn websites.

There are things that require more privacy. e.g. A person from a suppressed country who protest under a pen name now can be traced back

We can even give you more examples. People who hide their sexuality in the real world but open about it on the Internet, People who seek discreet medical help on public forums etc.

Let us demonstrate the issue by using one of their team member avatars.

Pay attention. We are going to use only the avatar URL to find the user related activity on the internet

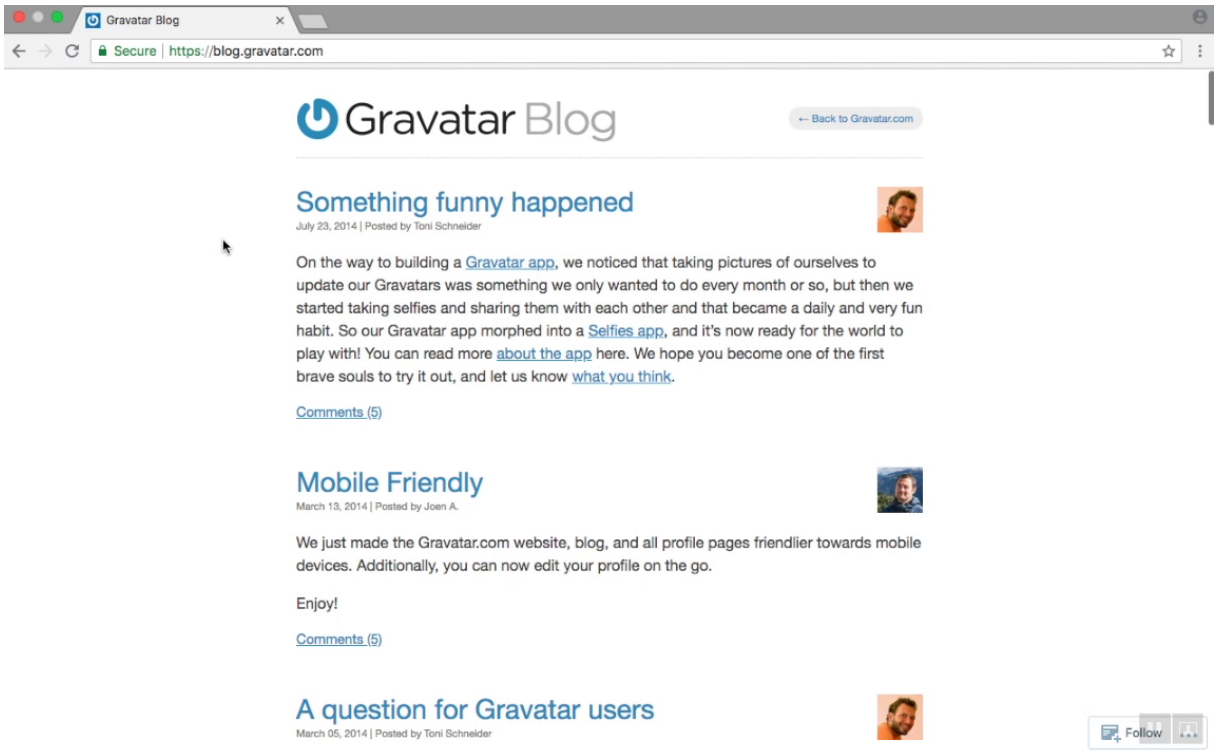


Figure 144: Toni's avatar on Gravatar Blog

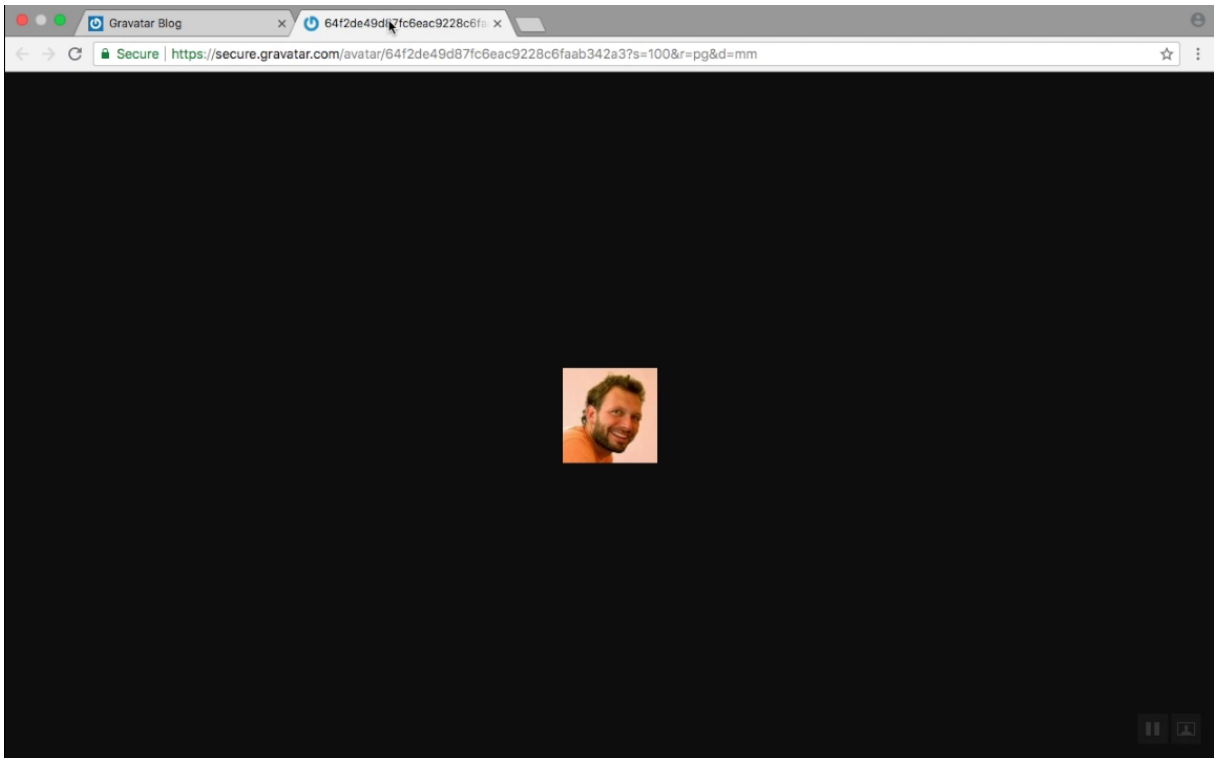


Figure 145: Copy avatar URL

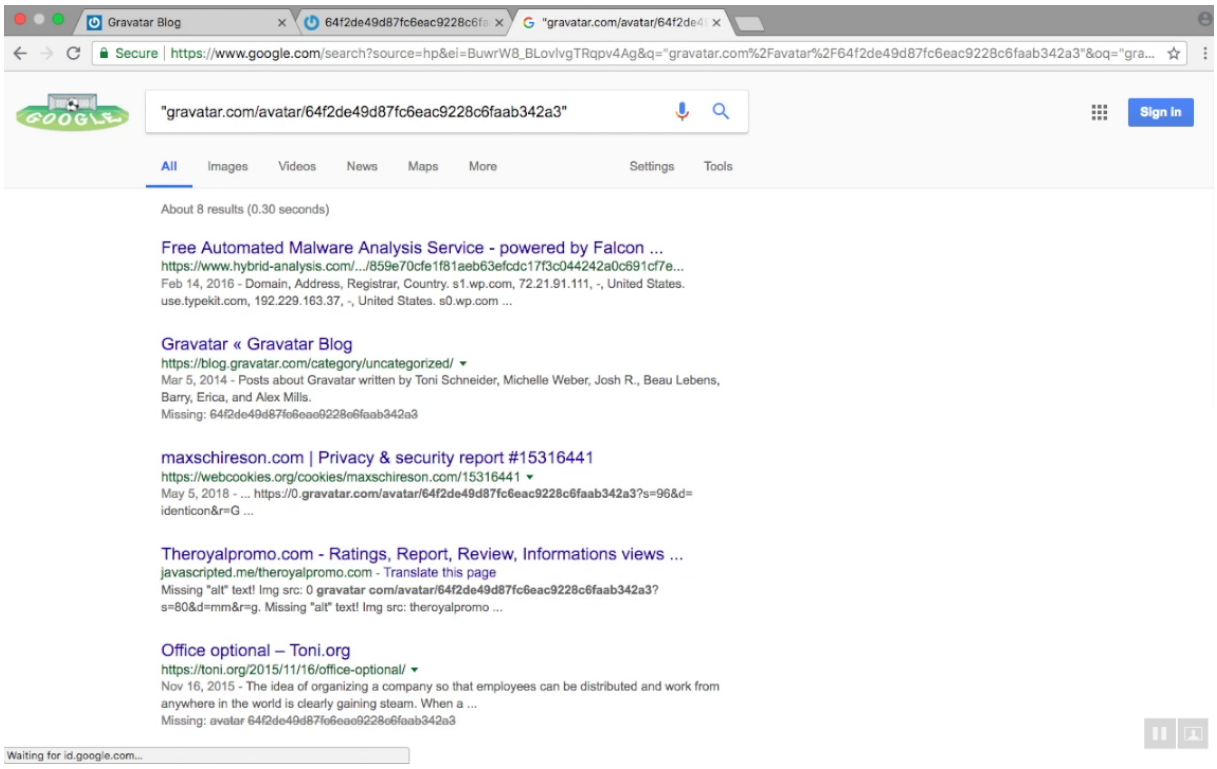


Figure 146: Google that avatar URL

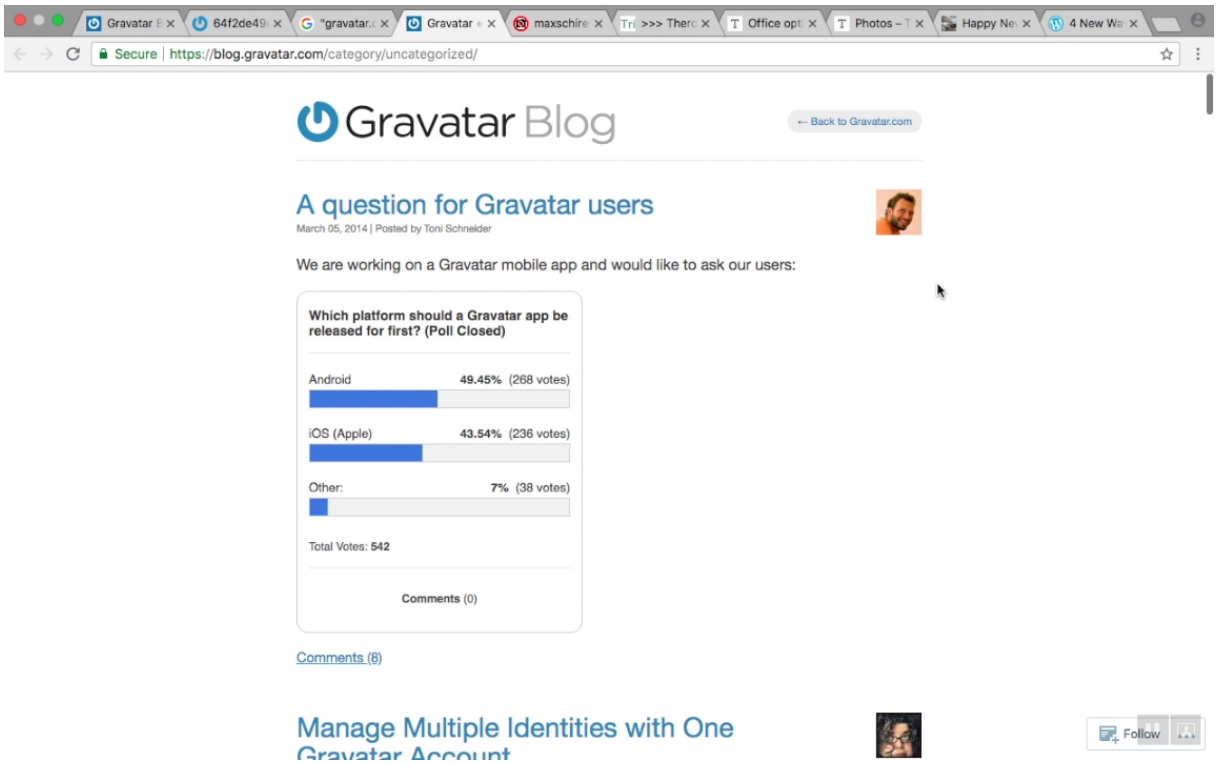


Figure 147: Valid Result 1: Article written by Toni on Gravatar blog

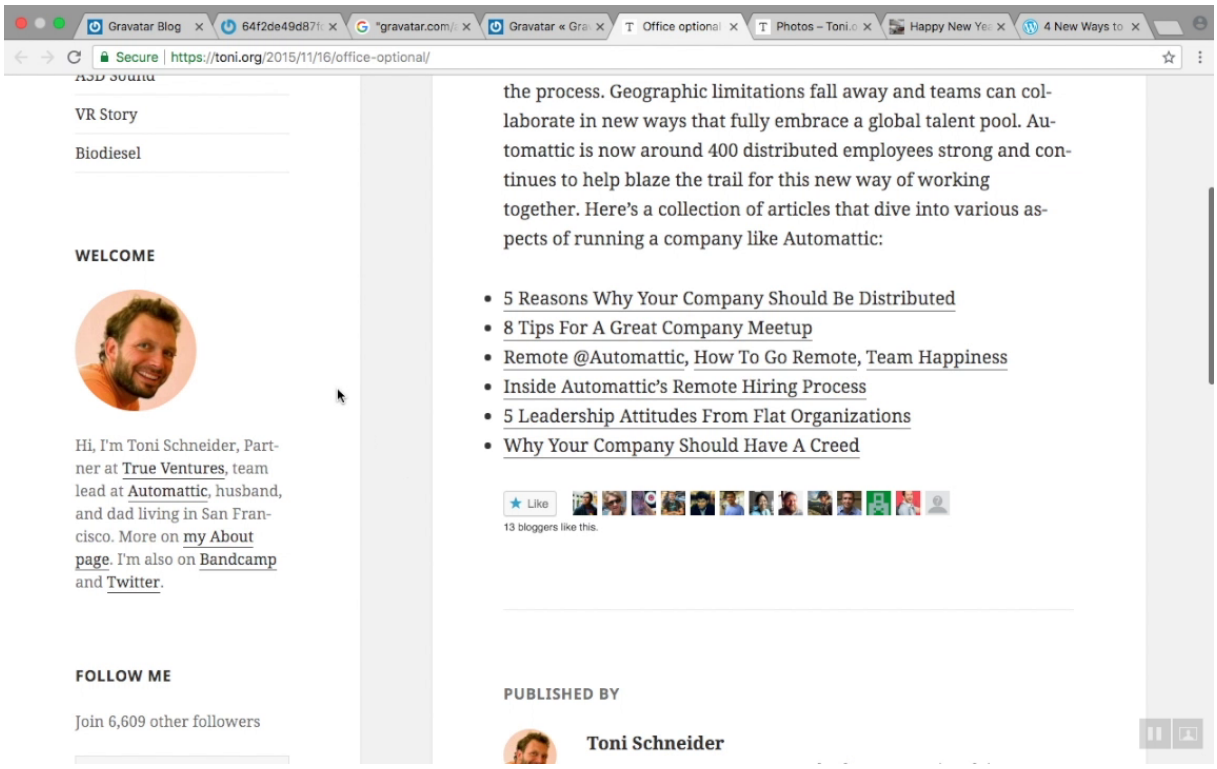


Figure 148: Valid Result 2: Personal Blog Of Toni

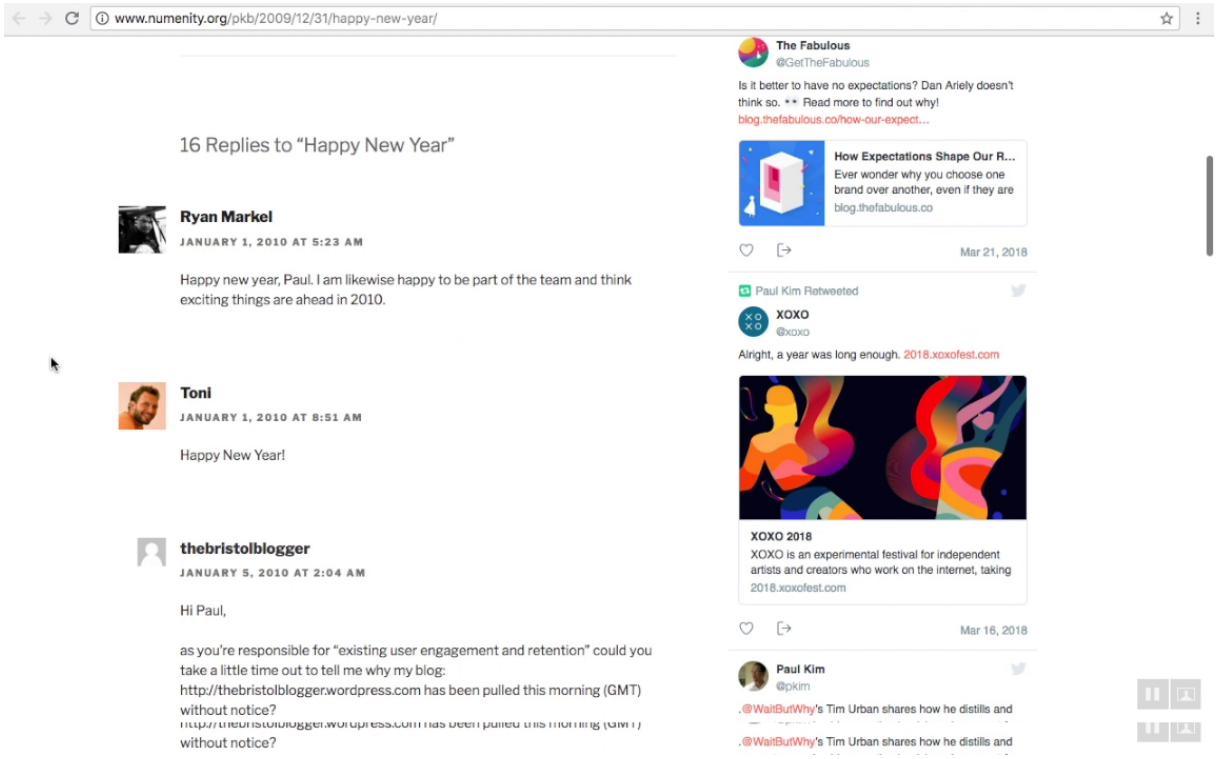


Figure 149: Valid Result 3: A comment posted by Toni on Numenity blog

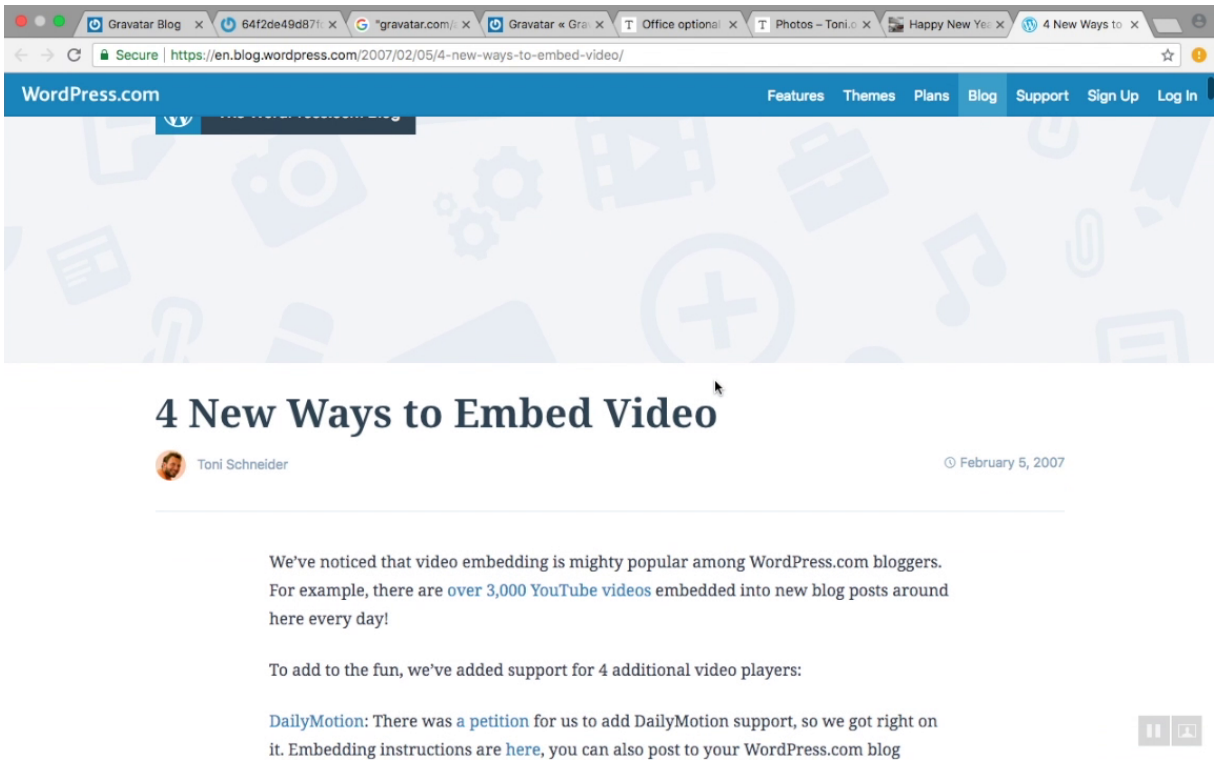


Figure 150: Valid Result 4: Article written by Toni on WordPress blog

Google indexed only certain pages. But if you build a web crawler only for that particular job, then you can have more results

Even if "Toni" change his name to "John" while signing up to a website or commenting on an article, the avatar URL going to stay the same since its linked to his email address. So he can be traced back

Again... We found those results, using only his avatar URL. not his name.

Government agencies can able to create full-fledged scanning tool only for this purpose.

This is what privacy is all about. People may think they are invisible on the internet. But they are not.

Now we know what you are gonna say.

"I have never heard of Gravatar before. So why should I bother?"

Well... we got news for you. The disturbing thing here is that It doesn't matter whether you have signed up for Gravatar or not.

Keep in mind, the subject of our discussion here is "Gravatar URL". Not "Gravatar Users"

If you have ever used your email address on a third party website for commenting or signing up, chances are your privacy is at risk.

This is because third-party websites have no idea whether you had signed up for gravatar or not. So they need to build the Gravatar URL for everyone using email hash.

If there is an avatar linked to your email address, then that avatar will be displayed. Else a default avatar will be displayed.

The blog on the next image contains 500+ users comments with avatars.

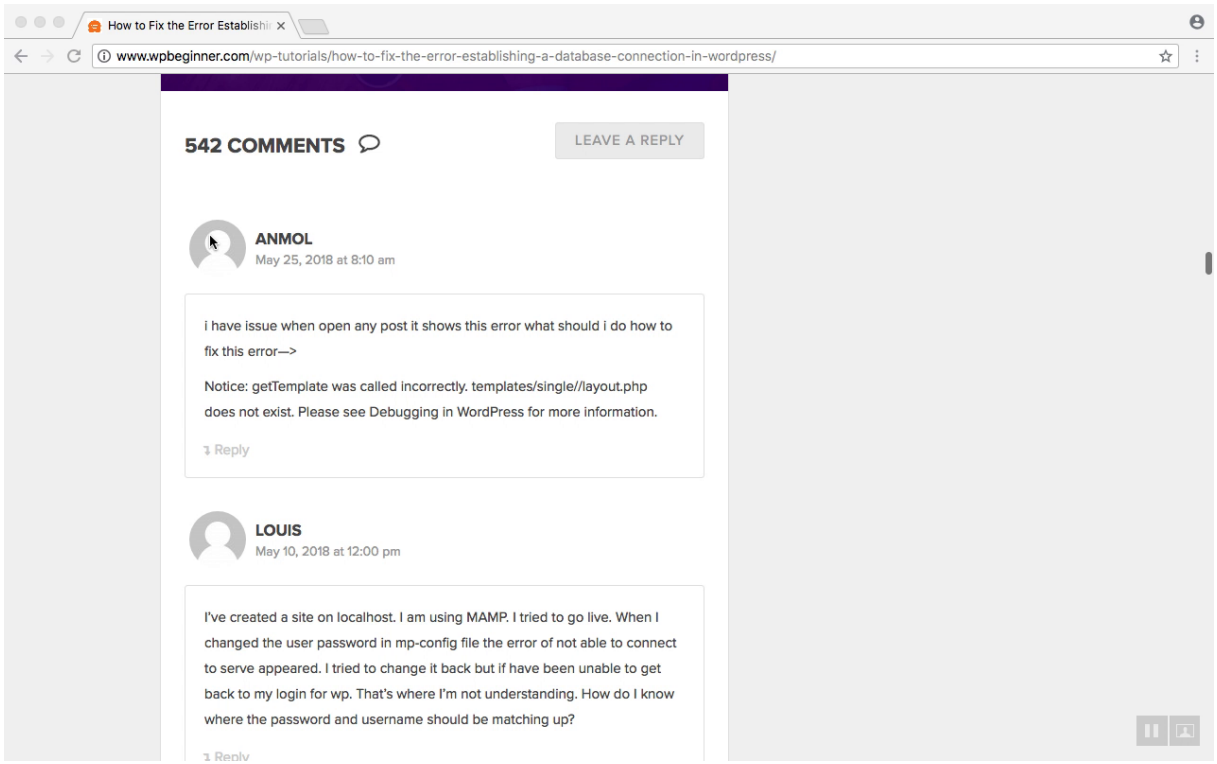


Figure 151: Blog Comments

The comments that have an avatar are the real “Gravatar” users. The comments that have dummy avatar are “Non-Gravatar” users.

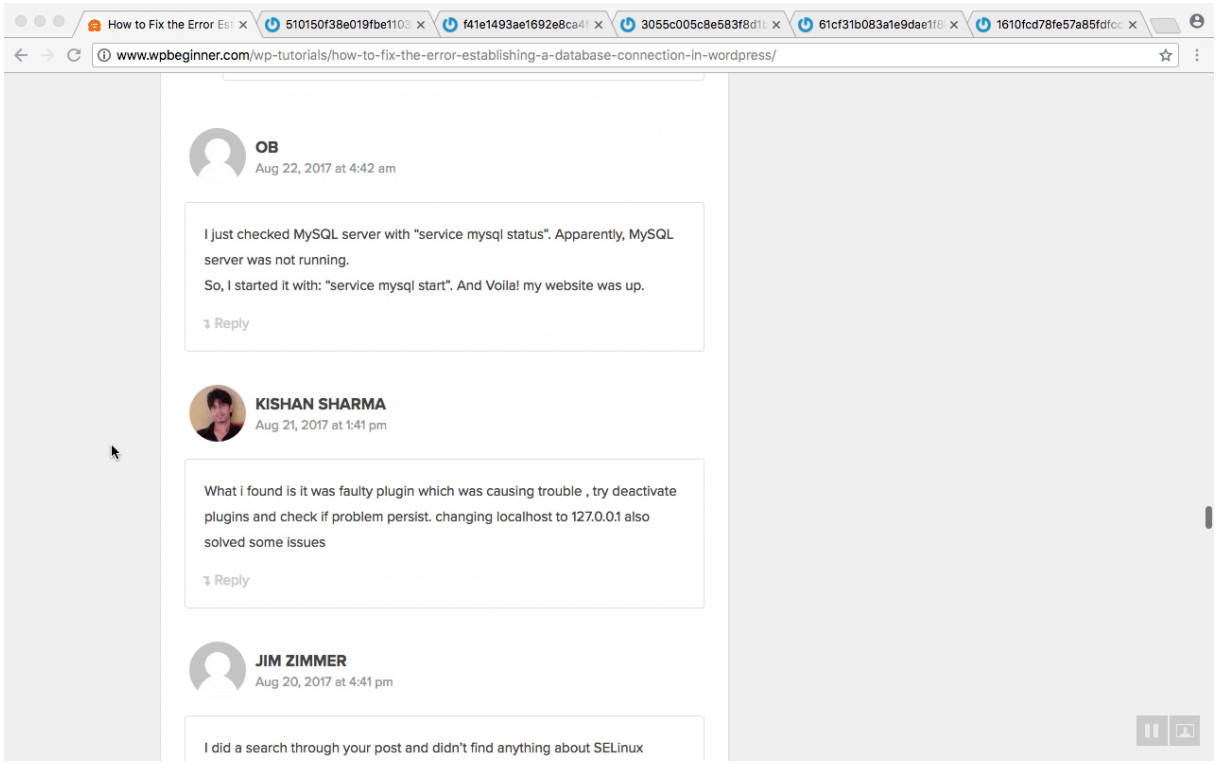


Figure 152: Non-Gravatar vs Gravatar Images

Pay attention to the “Non-Gravatar” user avatar URLs. Email addresses are still hashed there.

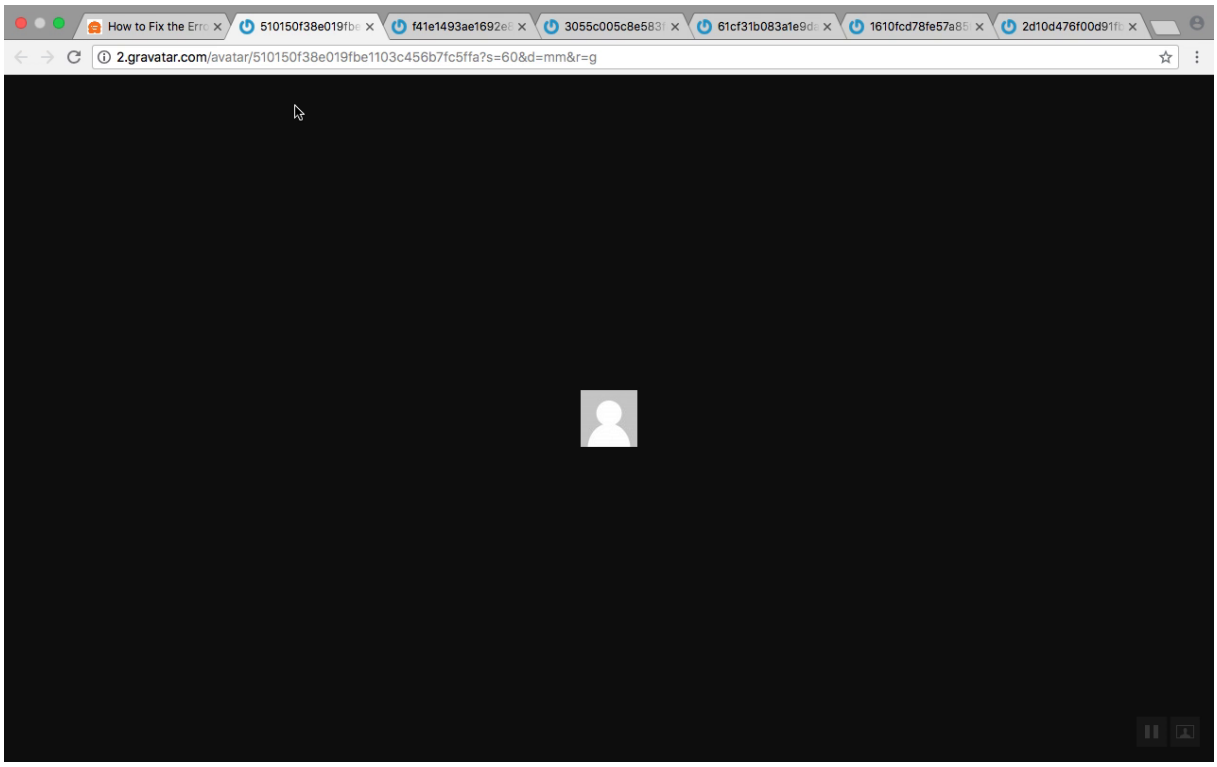


Figure 153: Non-Gravatar user URL

There may be few million gravatar users. But you can most likely find billions of gravatar URLs on the Internet.

For what its worth, We are not blaming Gravatar for this. Because the problem they solved is completely different. We are just pointing out the flaws in their system. [Gravatar privacy issue applicable only for the public pages that can be crawled]

"Signup with Google", "Signup with Facebook", or any other "Auth button" for that matter, none of these buttons going to help you in this case except our "Teleport" button.

Only our "Teleport" button can give you "better privacy" while compared to 100+ auth buttons

Because our "Teleport" button creates a new Dombox and the Dombox comes with a unique email address for each website. So your gravatar URL for example.com is not

going to be the same as example.net

Foundation

What is the definition of Dombox? Domain-based Isolated Mailbox right?

Isolation - That's the magic word here.

Let's ask Google to define "Privacy". Pay attention to the synonyms

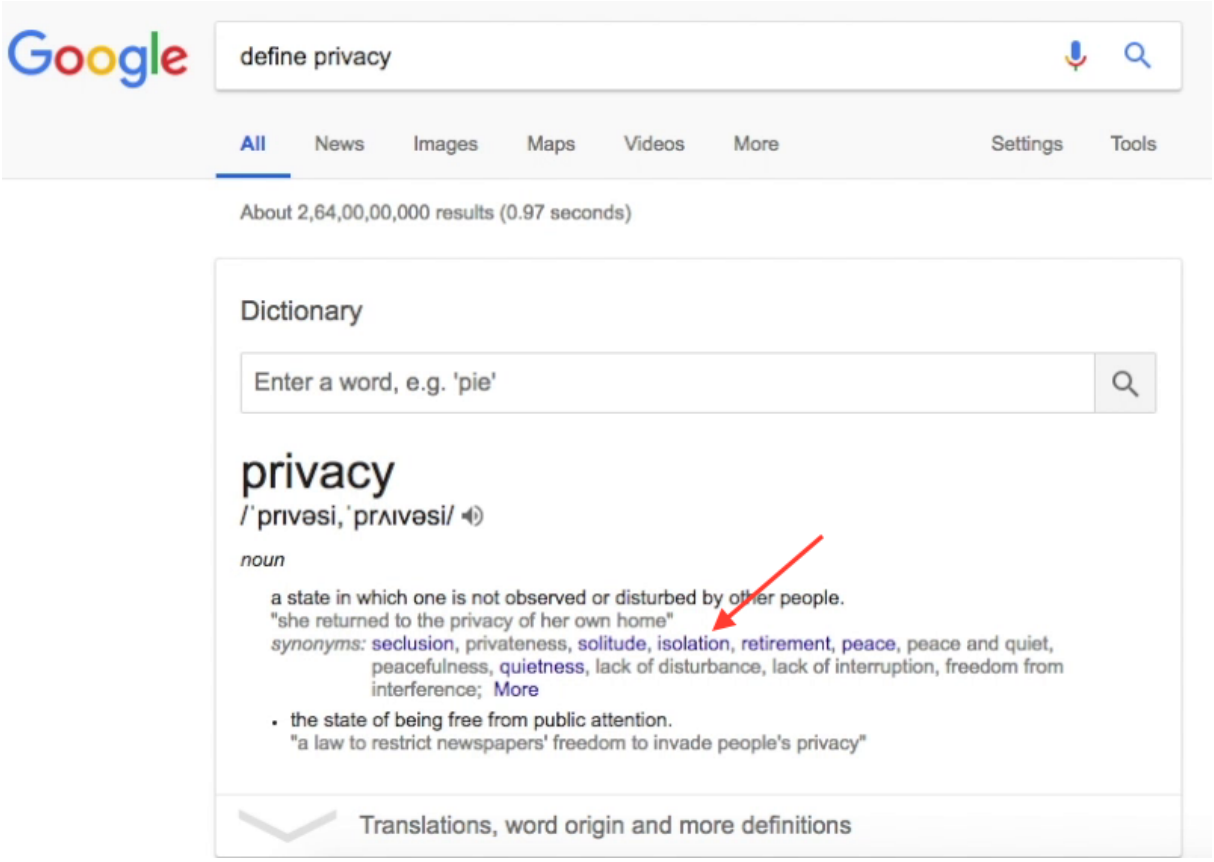


Figure 154: Define Privacy

As you can see in the last image, privacy and isolation mean the similar thing.

Now, If you do the math, one thing is very clear here.

> For companies like Google and Facebook, Privacy is merely a Feature. But for our company Dombox, It is the Foundation

Chapter 20: Benefits

Spam - There will be less spam on the Internet

Phishing - The phishing emails will be reduced a lot. Because if you signup to facebookmail.com using a Dombox mail address, the box won't accept any emails from facebook**e**mail.com unless it got whitelisted via SAD. So you cannot be deceived.

Homograph Attacks - This attack can deceive even highly technical people. Let us give you an example. Can you tell us what's wrong with this domain? => paypal.com. The character "a" is replaced with the Cyrillic character "а". If you need proof, copy those characters, go to google.com and then paste it into the search box. See the search suggestions. Unfortunately, Cyrillic characters are allowed in domain names. Our Domboxes are safe from homograph attacks[96]. Refer the last point why dombox is safe from homograph attacks. By the way, you can find Cyrillic characters in the Russian text. e.g. азитромицин

Malware - Since there won't be any spam emails, there won't be any malware emails too.

Organized - Your mails will be well organized. Each dombox acts as a dedicated folder for its domain. If you wanna fetch medium.com mails, you know where to go.

Relevant Search - You can get more relevant search results. If you wanna search some work related mails, just exclude "Domboxes" by unchecking it in the search field. Now, you will get search results only from the mails found under "Mailboxes" group.

Productivity - The world is gonna be at least a little bit more productive than what you have today.

Scamming - Innocent people will be saved from Lottery scam, Employment scam, Nigerian scam, Romance scam etc.

[96] https://en.wikipedia.org/wiki/IDN_homograph_attack

Control - In mail service like Gmail, others have control over you. In our mail service, you have the full control. You can decide who can mail you and who can't.

Rogue Websites - Some rogue websites that make a living by selling your data can't sell your data anymore.

Teleport - Teleport gives you quick signup and sign in. If we succeed, then that's gonna be everyones preferred mode of signup and login. So the traditional signup and login forms will become an option.

Privacy - Unlike other services, our "Teleport" button gives you full privacy on the internet.

Hacker Resistant - Hundreds of thousands of websites are getting hacked every year. But you would find only the popular sites on the news if they get hacked. Our Teleport button solves this issue. Even if your "Green Data" get stolen from a third party website, you are still safe. Because hacking this data is nothing more than crawling facebook profiles.

Competitor Resistant - You have built a successful online business. You have a lot of high profile clients. If your competitor uses a hacker to hack your website, they can steal the data, contact your clients anytime and hijack your clients by persuading them. So our Teleport button can protect your business. When you use our "Teleport" button, You are the only one who can reap the benefits.

Telescribe - Our "One-Click" subscribe button gonna save you some time since its "Double Opt-In" by default.

Pre-Signups - Budding entrepreneurs usually don't have enough money until they bring investors on-board. While building their product, they can now accept pre-signups via our Telescribe button without spending a dime.

Passwordless - "Teleport" button doesn't require a password. But if you have a highly sensitive website (e.g. Banking) you are welcome to ask your users for a password after successful authentication. In such cases, you can use "Teleport" as "Primary" authentication method for identifying user and "Password" as the secondary authentication method. You

can also use an alternative method like “Tokens e.g. OTP” for the secondary authentication method

Security - We do have plans to issue free SSL certificates to all of our “Portal Partners”. So the internet will be more secure than what you have today.

Unsubscribe Requests - Unsubscribe Requests are gonna be more streamlined. Our unsubscribe button found in the Dombox can help you automate the unsubscription process. Just click the unsubscribe button and we take care of the rest. Unsubscribe button also helps us to keep track of offending sites. e.g. If a site is our portal partner and keep annoying even after multiple unsubscribe requests, then they are breaching our terms and conditions. So the contract may get terminated. You already have full control (“Delete” and “make Offline” privileges) for non-partner boxes. So there is no need to depend on third party services for unsubscriptions.

Mailboxes - Google has a “Priority” inbox. Mails are decided by their algorithm. Outlook has a “Focused” inbox. Mails are decided by their algorithm. But we are giving you something better than that. The “Primary” box type. Mails are decided by you. Just use your primary box mail address only for conversational emails and all emails will be considered as “Priority” over the emails found in Domboxes.

Domboxes - We are also planning to bring a “Priority” tab feature for “Domboxes”. You can set priority for each and every dombox. The Priority value can be 1 to 1000. The default is 500. Let’s say you have 5 domboxes. a.com, b.com, c.com, d.com and e.com. If you don’t set any priority, then all boxes have the same priority 500. So the emails will be ordered as usual. Let’s say you set the priority value “1” to “b.com” and “1000” to “d.com”. Now the emails will be ordered like this. b.com, a.com, c.com, e.com, d.com

Email Misuse - No one can misuse your email address by submitting the form in third party websites. This is because a “Dombox” needs to be created first either via “New Dombox”, “Teleport” or “Telescribe” button with your knowledge to receive emails.

Confirmation Mails - There is no need for confirmation emails. Because “Isolated Mailboxes” should be considered as “Double Opt-In” by default. {Refer the last point for more info}

Whitelist Request - Since a "Dombox" is owned by both consumer (Read & Delete Privileges) and business (Write Privilege), there is no need for whitelist request. In other mail services, a website owner usually requests their users like this. "Please add contact@example.com to your address book to ensure delivery into your inbox"

Inboxing - Most businesses these days looking for an answer to this question. "How to get our emails delivered to the user inbox instead of ending up in the spam folder?". "Dombox" is the perfect answer to that question. Dombox not only helping the consumer to achieve zero spam but also helping your business to reach the user inbox without any issues. When you send emails to an address like @gmail.com, your domain is actually 1 in a million. So there is gonna be trust issues. But when you send emails to the "Dombox" created for your domain, we were actually expecting your emails. You get exclusive privilege there. When a consumer creates a Dombox for your domain, that establishes your domain's credibility. If your domain passes all our 5 layer checks, then your emails will always get delivered to the user inbox unless your mail gets caught via our "Anomalies" filter.

Reversible - In other mail services, the spam you are getting always will be in ascending order. If you receive 10 spam emails today, 5 years from now you are gonna get at least 100. But in our mail service if you receive 100 spam emails in your "Primary" box, you can go back to "zero spam" easily by isolating the websites you already signed up and then restricting your primary box.

Mail Score - Since we bring transparency via Mail Score, that's gonna force the website owners to configure those layers. That means you are gonna have better mail experience than before even if you use other mail services like Gmail. i.e. We are helping other mail services indirectly

BotNets - BotNets contribute a lot to our everyday spam. Some botnets are capable of sending spam up to 90 Billion spam emails per day. Our system is probably the only system that is safe from such BotNets.

Spam Laws - Spam laws are enforceable only within a country. If the spammer is from some other country, its hard to get justice. But our system is a global system. If we succeed, there won't be a need for spam laws in the long run.

Bandwidth - Half of the Internet bandwidth is being used to carry spam emails. If we succeed, plenty of Internet bandwidth will be freed.

Storage - We are trying to remove the spam folder completely in the long run. So plenty of storage space will be saved.

Statistics - If you are business owner, you wanna know how many people opened your mails. This is a privacy issue. When someone sends you an email, they are implicitly saying "Reply me when you have time". So email is a fast but slow tool. For example, if Gmail adds those read receipts like you see in whatsapp or messanger tomorrow, that would create a massive backlash due to privacy concerns. But our system is dual-sided system. Mailboxes and Domboxes. Since dombox addresses used only for website related mails, we can offer the crystal clear statistics to businesses directly. However, you need to become our Portal Partner and accept few terms. e.g. You will not use our API for getting the "read status" of conversational mails found in your domain dombox.

STRIPTLS attacks - Domboxes can be protected from STRIPTLS attacks since they are isolated. So it can offer better security.

Prototype

> https://www.youtube.com/watch?v=VK2eSfCurx4

Amendments

In this document, we mentioned website owners need to prove that their mails MUST pass all five layers to become our portal partner. We believe some layers are complicated to configure for non tech-savvy users. We don't want to put the burden on the webiste owner's shoulder and we want our system to be able to adopt easily.

So we change that requirement to only two layers. Authroization Layer (SPF) and Alias Layer (SAD). So to become our portal partner, all incoming mails MUST pass Authroization Layer (SPF) and Alias Layer (SAD). We don't mandate the other three layers. How-

ever, we highly recommend other three layers, so your incoming mails can get full 5 marks for Mail Score and looks trustworthy infront of reader's eyes.