The security risks of unverified and recycled email addresses

Bachelor's Thesis Computing Science

Tea Coros
s1020923

November 9, 2022

First supervisor/assessor:
Professor Bernard van Gastel

Second assessor:
Professor Gunes Acar

Radboud University

Abstract

Unverified and recycled email addresses are a security risk for user accounts on all types of websites. We have analysed many popular websites for their levels of security in the context of email addresses, two factor authentication and password reset policies. A significant number of them allow users to use unverified and recycled email addresses which allows for an account takeover attack. Mitigations for these attacks can be implemented based on the services websites provide. For this we provide a decision tree that can help websites make the right choice in order to achieve a minimum level of acceptable security.

Contents

Chapter 1

Introduction

Email addresses are used by almost all websites nowadays as a way to identify and authenticate users. If an email address is not used directly within a website, for example instead of a username, it is still likely connected to the website in case a user forgets their password. Because of an email address's relevancy to any user's online activities, it is of utmost importance to keep an email account secure. Unfortunately, there are many ways in which this can go wrong, as we will explore from here on out.

1.1 Goal

The main goal of our research is to find all security risks due to the use of unverified and recycled email addresses and to find mitigations for these risks. We will find the causes and consequences of the most dangerous risks associated with unverified and recycled email addresses. Thus, we will explore how a compromised email address would effect the security of a user account. Solutions should not only be done through sever-side checks but also through requesting additional verification from the users. We will also look into user behaviour and how some users may react to certain changes in website policies.

It is also in our interest to warn the general public of the security risks we have discovered. Keeping users informed will help prevent attacks in and of itself [1] and thus it is also in the interest of the user's online safety. It is much easier for users to understand why certain policies are used when they also understand the possible attacks they prevent. This will also help with encouraging the use of optional safety features by users.

1.2 Scope

The term "unverified and recycled email address" will be referring to an email address that is either not valid, has been used by a different user in the past, or is in danger of being compromised due to issues with its domain name. An address that is not used by anyone will be seen as an invalid email address. The recycling of email addresses may also occur when a domain name owner considers that a user should no longer have access to an email account, for example due to inactivity. We consider an email address compromised when the rightful owner of the email address no longer has confidential access to the email account. We will not focus on users that have given away their email addresses by choice, through for example password sharing.

Security risks are comprised of the possibility of losing key components of security, namely confidentiality, integrity and authenticity. Within this context, we will mostly focus on confidentiality and authenticity.

1.3 Contributions

Firstly, we aim to bring the security impact of unverified and recycled email addresses to light. Based on this, we have created mitigations in the form of policies and regulations for websites. These policies and regulations are based on the best industry standard, where we will take the example of a company like Google in regards to their security related policies. Along with these policies we have created a decision tree for the specific use of companies and website owners in order to help them judge how they can best handle user policies regarding the validation of email addresses. These will provide a recommended minimum level of security in order to keep users' accounts secure in this context.

1.4 Approach

To achieve our goals and create our policies and regulations we have first analysed policies used by 34 different top websites.

These websites were chosen first and foremost for their number of visitors as of the time of this paper. These websites are generally owned by some of the largest companies in the world. We have excluded subdomains of the top websites from this list as they do not provide additional relevant information regarding security practices. However, other websites were added based on their relevancy to the issue of unverified and recycled email addresses.

Along with these policies we have created a decision tree that websites can use in order to improve their own policies. The decision tree will evaluate based on the likelihood of attacks and the loss such an attack would cause for users. This decision tree will help companies find mitigations so their systems are sufficiently protected against unverified and recycled email addresses.

Chapter 2

Relevancy

The importance of unverified email addresses became apparent to me personally while creating an account for the website `tumblr.com`(Tumblr). When first discovering this issue, I created a brand-new email address from the provider `mail.com` using one of their available domain names. While trying to register for a Tumblr account, I discovered that my freshly created email address was already in use within Tumblr's system.

Tumblr provides a convenient login option where a login link is simply sent to the user's email. Normally, this would not effect the integrity of an account; but in this case, logging in becomes even simpler for an attacker. It allows any attacker to simply use the "magic link" option while logging in, through which Tumblr sends you a link containing a corresponding session cookie for your account. If this were not the case, an attacker would have to manually change the password of the compromised account, which may alert the original user to the suspicious activity. Here, extra security could be added by making use of some form of two-factor authentication. This could, for example, be reproducing a code sent through a text message or answering security questions in order to verify the identity of the user.

Once I checked that the email address belongs to an actual account, I was able to simply log into that Tumblr account without ever knowing or having to change the password. This is catastrophic for the security of that account.

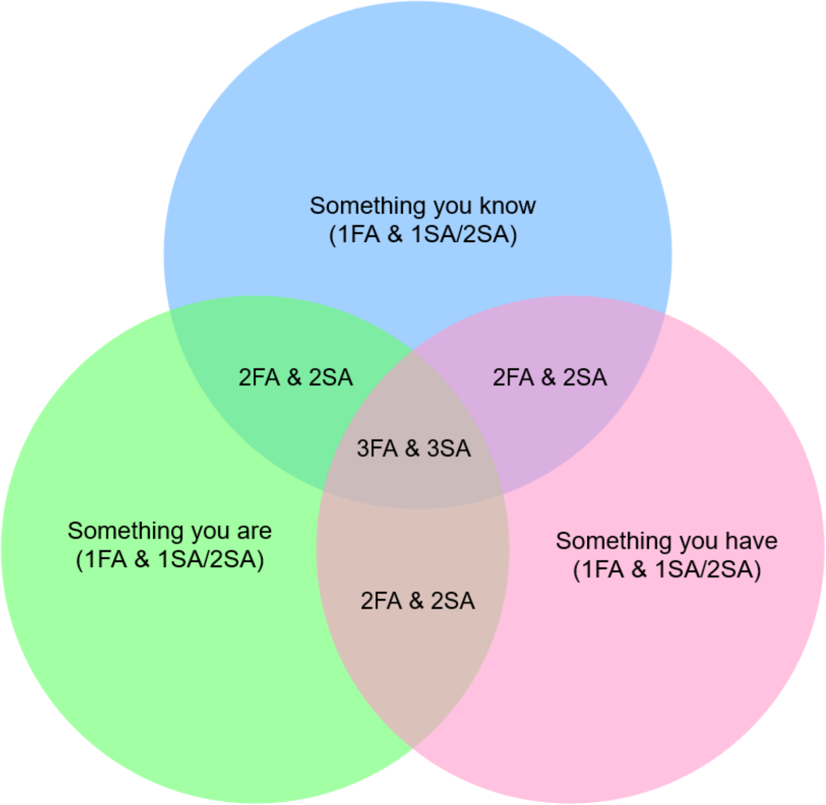

Figure 2.1: Difference between factor authentication and step authentication

2.1 Account takeover

In the case of Tumblr, one did not even have to reset the password in order to gain access to an account. On most other websites, one would need to reset the password in order to actively get into an account. At this step, a form of two-factor authentication would be introduced in order to verify the identity of the person requesting a password reset. In the case that only two-step authentication would be used, a serious attacker would only be minorly inconvenienced. In most cases this type of additional security is omitted. This can be on the basis that an email address is not easily taken over, but as we have have seen above, one cannot always rely on this.

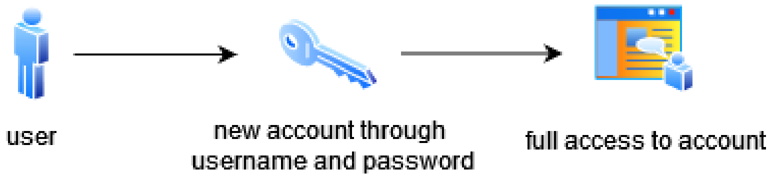

Figure 2.2: Single-factor and step verification for account creation

2.2 Two-step authentication

Two-step verification, also commonly called two-step authentication, requires two methods of authentication. A common way this is done, is by making sure the user has access to two accounts on different platforms in order to log into one account: two things the user knows. A specific example would be knowing your email password and your bank password. This method is not often applied to two things the user has or is, as it would be more difficult to implement, although the term does incorporate this type of use.

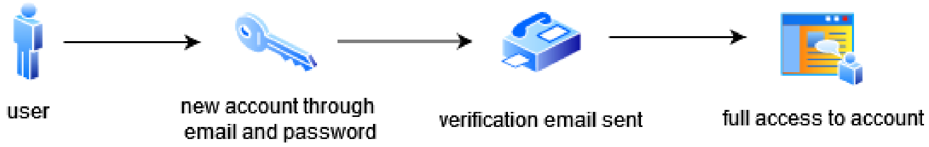

Figure 2.3: Two-step verification for account creation

2.3 Two-factor authentication

The concept of two-factor authentication is based on the three methods of authentication: something you have, something you know and something you are. Two of these methods are combined in order achieve two-factor authentication, but unlike for two-step verification, the methods must be different from one another. This provides additional security as different aspects of security are involved. We can see it as a subset of two-step verification.

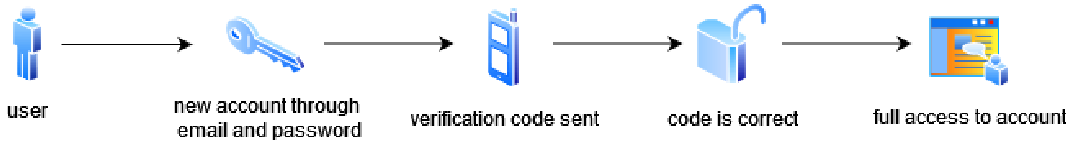

Figure 2.4: Two-factor authentication for account creation

2.3.1 Weak two-factor authentication

The most well known form of two-factor authentication is weak two-factor authentication, which generally makes use of a software token. Software tokens can be anything from security questions to emails to SMS messages, which can all be tampered with remotely. [2] Security questions can be answered with enough information on a person, email addresses can be taken over in different ways and SMS messages can be intercepted. All these methods combine things the user knows or owns in order to provide an additional layer of security. However, when these methods are not foolproof, the security they offer may also become flawed.

2.3.2 Strong two-factor authentication

In order to combat some of these issues we have strong two-factor authentication which makes use of a hardware token. These are usually in the form of an USB-stick that is solely being used in order to authenticate users, meaning the second factor of authentication in this case is always something users own. These tokens are not something that can be intercepted easily, as one would need physical access to a location in order to be able to obtain one. Thus the physical security this provides is something that can not be easily guaranteed in other forms. These hardware tokens are not used as commonly as it would be difficult to provide every user with a physical token in order to log into a service. Additionally, they may be difficult to operate for less tech savvy users, especially when they do not see the benefit of the additional security provided. While it may change in the future, right now it is unrealistic to expect the general public to use a hardware token for everything they log into.

Because of this, it is relevant that weak two-factor authentication, most notably when performed through email, remains as secure as possible.

2.4 Phishing

Most research regarding the security of email accounts is related to phishing. This is indeed the most common attack as it makes use of the social engineering in order to get access to any kind of account a user may have. Because of this, many institutions including the Radboud University, have taken many precautions regarding training their personnel to recognise phishing attempts. In the case of these emails, awareness is one of the best defences a user can personally have. [3]

Another way to defend against these types of emails is to make sure that they never get to the user in the first place. This is usually achieved by sending suspicious emails directly to a spam folder, which also leads to users being weary of these emails. Nowadays, the detection of these suspicious emails is more sophisticated, giving very consistent results [1]. This again helps with the identification of phishing attempts for users.

The mitigations for phishing are well known and implemented consistently at this point, thus making phishing emails less of an overall risk for users.

2.5 Data leaks

In early 2020 a data leak occurred where phone numbers, Facebook IDs, full names, locations, birth dates, and at times also email addresses. [4] All this information is crucial to the privacy and security of users. Phone number and email address combinations are especially dangerous as they can be used in order to avoid the security of weak two factor authentication.

An attacker could simply go through the list of email addresses where one can find a phone number tied to that account and try to take over the email address when it is no longer active. This means that one can ask for a new password for any site and then use the email for confirmation. Due to having the required phone number, one can use the attack described in Section 2.3.1.

Such data leaks occur on a regular enough basis for such attacks to be possible. If the right combination of credentials is leaked these types of attacks would have catastrophic effects not only on a user's privacy but also to the security of multiple online accounts.

Chapter 3

Analysed websites

Below we have analysed the security of the accounts of the most popular websites used by English speakers. [5] The popularity is based on the number of visitors a website has. We have chosen to exclude sites where very few visitors actually create an account, meaning websites similar to `wikipedia.org` and `bit.ly` are not part of the list.

For comparison we have also chosen some less popular websites that may be significant. We have chosen to have a look at `marktplaats.nl`(Marktplaats) which is a popular Dutch website that is similar to `ebay.com`(Ebay) and `craigslist.org`(Craigslist), in order to judge if there is a difference in their approach to security. Furthermore, we have also taken a look at `protonmail.com`(Proton) as they advertise their email services to be very security orientated. Finally, we have also added Tumblr to our list, as it is an example of a website which is clearly vulnerable to our attack.

3.1 Categorisation

In order to be able to compare websites' security in the context of email addresses, we have decided upon a few metrics that needed to be checked.

Firstly, we of course consider whether or not a website provides email verification. In this case we only count when mandatory email verification in order to access a website. Whenever the verification of the email address can be skipped, it does not provide additional security against attackers, as someone who has lost access to their email can still make an account. When there is no mandatory check, we check if email verification is needed to access any features of the website. If this does not hold as well, we have concluded that the website does not provide email verification.

Secondly, we check which login methods are available for users. We have distinguished between the use of email addresses, usernames, mobile numbers and third party authentication. We have chosen these options as they are the most common ones within websites. Almost all websites use one of these options if not multiple.

Thirdly, many websites choose to offer third-party authentication, where a user may login using the login credentials of a different website. With this, trust is placed in the third party that they will offer security to users who choose to create an account using this option. This transfers the risk to a usually more trusted website, like Google or Apple. It is also sometimes the case that the third-party authentication that is offered is from a parent company, though for simplicity we have chosen to still refer to this scenario as third-party authentication. In the table, the third-party authentication options which are offered are noted in the parentheses.

nr.	Name	Email Verification	Login method	Third-Party Auth.	Password Resets
1	google.com	yes	email/mobile	no	email/mobile
2	youtube.com	yes	third-party	yes (1)	third-party
3	facebook.com	yes	email/mobile	no	email/mobile
4	twitter.com	yes	email/mobile	yes (1/apple)	email/mobile
5	yahoo.com	yes	email	yes (1)	mobile
6	pornhub.com	restricted access	username	no	email
7	instagram.com	yes	email/mobile	yes(3)	email/mobile
8	xvideos.com	restricted access	email	no	email
9	xnxx.com	restricted access	username	no	email
10	amazon.com	yes	email/mobile	no	email/mobile
11	live.com	yes	email	no	email/mobile
12	netflix.com	no	email	no	mobile
13	whatsapp.com	no	mobile	no	mobile
14	reddit.com	no	username/email	yes(1/apple)	email
15	bing.com	yes	third-party	yes (11)	third-party
16	xhamster.com	restricted access	username	yes(1)	email
17	ebay.com	yes	email/username	yes(1/3/apple)	mobile
18	twitch.com	no	username	yes	email/mobile
19	linkedin.com	yes	email/mobile	yes(1)	email/mobile
20	msn.com	yes	email	yes(11)	email/mobile
21	pinterest.com	no	email	yes(1/3)	email
22	fandom.com	restricted access	username	yes(1/3/18/apple)	email
23	quora.com	yes	email	yes(1/3)	email
24	github.com	yes	username/email	no	email
25	youporn.com	yes	username/email	yes(6)	email
26	paypal.com	yes	email/mobile	yes	email
27	wordpress.com	no	username/email/link	yes(1/apple)	email
28	booking.com	no	email/link	yes(1, 3, apple)	email
29	craigslist.org	yes	username/email/link	no	email
30	spotify.com	no	username	yes(1/3/apple)	email
31	marktplaats.nl	yes	email	yes(1)	email
32	protonmail.com	no	email	no	email/mobile
33	redhub.com	restricted access	username/email	yes(6)	email
34	tumblr.com	no	username/link	no	email

Table 3.1: Authentication method per website

Lastly, we have also noted in which way an account can be recovered in the case of a user no longer being able to recall their password. From what we observed this is either done through email addresses or mobile number checks. For this, one either needs access to the email account or mobile phone number that is attached to the account, in order to either receive a link or a code for a new password.

nr.	Name	Two-step	Something you know	Something you have	Relevant information
1	google.com	yes	yes	yes	mandatory
2	youtube.com	yes (1)	yes (1)	yes (1)	only through google
3	facebook.com	yes	no	yes	
4	twitter.com	yes	yes	yes	
5	yahoo.com	yes	yes	yes	mandatory
6	pornhub.com	no	-	-	
7	instagram.com	yes	no	yes	
8	xvideos.com	yes	no	yes	
9	xnxx.com	no	-	-	
10	amazon.com	yes	no	yes	
11	live.com	yes	yes	yes	
12	netflix.com	no	-	-	
13	whatsapp.com	yes	no	yes	
14	reddit.com	yes	no	yes	through google
15	bing.com	yes (11)	yes (11)	no(11)	only through live
16	xhamster.com	no	-	-	
17	ebay.com	yes	no	yes	
18	twitch.com	yes	no	yes	
19	linkedin.com	yes	no	yes	
20	msn.com	yes (11)	yes(11)	no(11)	only through live
21	pinterest.com	yes	yes	no	
22	fandom.com	no	-	-	
23	quora.com	yes	yes	no	
24	github.com	yes	no	yes	
25	youporn.com	no	-	-	
26	paypal.com	yes	no	yes	
27	wordpress.com	yes	no	yes	
28	booking.com	no	-	-	
29	craigslist.org	no	-	-	
30	spotify.com	no	-	-	
31	marktplaats.nl	yes	no	yes	mandatory
32	protonmail.com	yes	yes	yes	
33	redhub.com	no	-	-	
34	tumblr.com	no	-	-	

Table 3.2: Two-step authentication per website

We have also checked the websites for two-step authentication. From our table it is possible to see which websites also offer two-factor authentication. On almost all websites one needs a password to login, meaning that if a site offers “something you have” as a security factor, it also offers two-factor authentication. We have noted when a website makes two-step authentication mandatory, as this is a strict security policy. Whenever a website only offered third-party authentication, it would naturally also inherit the policies of these third parties. All this information, gives us an insight in which security options each site provides their users with, and thus giving us the maximal potential security a website has to offer.

3.2 Case studies

In this section we will describe notable information about certain websites. From here on out we will use a websites domain without their top-level domain to refer to them as their full domain has already been listed above.

3.2.1 Google.com

Google is a great example to follow at least in terms of security as they have mandatory two-factor authentication for all their users. For convenience, Google offers their users the possibility to remember a device, giving them the convenience of skipping two factor authentication when they are using a familiar device. It is also notable that they offer email accounts themselves, where users can set up a recovery email address that is provided by a different website. This secondary email address is also verified before it can be used for account recovery.

3.2.2 Facebook.com

Facebook has an easily accessible option for recovering your account in the case that your email address gets taken over. However, when you choose to log out for the first time, an email is sent to you with a Magic Link for you to easily log back in. Facebook may not realise that this can be exploited immediately whenever an email address gets taken over. Although, if that link contains a session cookie that is only valid for a very short amount of time, this attack would be mitigated in most cases.

3.2.3 Pornhub.com, Xvideos.com, Xnxx.com, Xhamster.com and Youporn.com

Some of the most popular pornographic websites do not offer two-step authentication. Most also have questionable practices in regards to password resets policies. One should also keep in mind that these types of websites often offer paid premium services, but do not usually provide additional security that would keep the account for which the purchases are made more secure. Furthermore, most pornographic websites have two types of accounts, one is for viewers and the other is for content creators. Usually viewer accounts lack security options, while creator accounts have strict requirements for their users. These segregation is understandable as most viewers are not also content creators on these websites.

3.2.4 Google.com, Yahoo.com, Live.com and Protonmail.com

All mail services within the list make serious attempts at security. They also tend to notify users of spam and warn against phishing. The only factor that may be seen as a risk is the fact that email addresses are relatively quickly recycled if left inactive. Most sites recycle a new account within a week of inactivity, or after six months to a year of inactivity for accounts older than one week. This quick recycling leaves many other accounts that are reliant on a specific email address vulnerable. On the other hand, changing policies to postpone recycling would cost of storage space as well as the availability of many email addresses.

3.2.5 Reddit.com

We noticed that Reddit is one of the few websites that does not explicitly require an email address to sign up, meaning that a user can permanently lose their account if they forget their password without adding an email address. This makes it more likely that a lot of accounts are lost. On the other hand, Reddit is more similar to a collection of forums where users may want to to post anonymously. Because of this, email-address-free accounts are used as throw-away accounts as to keep other private information from being linked to a person's identity.

3.2.6 Pinterst.com

Pinterest is the only site on the list that only makes use of email verification when a user wants to set up two-factor authentication. Most other websites either do not bother or limit the functions that a user can make use of on the site when their email address is not confirmed, but here a user only needs their email address if they want additional security. This means that users may choose either minimal security or maximal security with little in between.

3.2.7 Twitch.com

Twitch allows users to only verify their account with a phone number. While they highly encourage verifying an email address as well, it is not necessary. This does not necessarily take security away, as it means that users are not always susceptible to email take over attacks.

3.2.8 Ebay.com

Ebay allow you to sign in without a password if you choose to use a verification code that would be sent to you through a text message.

3.2.9 Booking.com and Wordpress.com

Booking and Wordpress also use magic links, making them vulnerable to the same type of attack that can be used for Tumblr.

3.2.10 Craigslist.org

Craigslist gives its users the option to have a passwordless account which allows users to always only use a magiclink to login. This would be very dangerous considering our attack as passwordless users may easily permanently lose their Craigslist account in the case of email address recycling.

3.2.11 Protonmail.com

In the case that one does not set up a recovery email or phone number, Proton warns you that it will be impossible to get your account back in the case of you forgetting the password. This does mean that they choose to always guarantee security, even if some users may lose their account. On the other hand, it is notable that when a recovery email is set, it is not required to be verified in order to be used.

3.2.12 Github.com

Github also warns its users that accounts with two factor authentication may not be able to be recovered if the users forgets their password and losses access to their phone.

3.2.13 Apple.com

Apple is not in the top visited sites but does offer third-party authentication that is quite popular. People with apple devices have the option to login with AppleID, which is automatically linked to their apple devices. this provides sufficient security in most cases.

Chapter 4

Model

Our final model takes the form of a decision tree. This tree takes many factors into account in order to give an appropriate level of security to website users. As we have seen from the tables in Chapter 3 there are different options for providing security, where some are more effective than others. Below, we analysed the most important factors that are related to email address security. Further on, we have analysed the most common mitigation we have encountered.

4.1 Variables

We have analysed many different types of websites where we found some trends regarding their approach to security based on different services they offer. These different security approaches were based on the services different websites offer. Additionally, we have also judged which types of websites could tighten their security, again based on their services.

- Websites that handle *monetary transactions* like Paypal or Google Pay should be protected thoroughly. They may store money and handle transactions between users, because of this losing an account could even lead to losing all the money a user had connected to an account. This is would be catastrophic for the user as well as for the reputation of the website.
- Websites which others depend on for security, through either *email authorisation* or more generally *third-party authentication* should also be as secure as possible. If one of these sites has a vulnerability, it would mean that all other websites that allow third-party authentication through it would be compromised. This would also hold if the website is an email address provider.
- *User memberships* should be protected by websites, as whenever a user would lose access to an account, that user would still be paying for a service they do not have access to.
- *Business* related websites, like Twitter and Linkedin, should be relatively secure as an account takeover may influence the reputation of a user. The monetary loss is generally not as direct as in the situations above, thus security can be more lax.
- *Social media* where reputations are relevant should also be protected similarly to business websites. Generally, there is less that users could lose in the event of an account takeover, as the damage is limited to followers and possibly a sponsorship.

- The *popularity* of a website is in practice somewhat relevant, but in our model we have assumed that all websites should provide adequate security regardless of their number of visitors.

4.2 Actions

We will take the information we have gathered from the websites we have analysed in order to create a ranking of security measures that can realistically be taken by websites. These will be the nodes or actions in our decision tree.

- mandatory physical token use (not applicable)
- mandatory two-factor authentication
- mandatory two-step authentication
- optional two-factor authentication
- optional two-step authentication
- email verification
- restricted access

We have chosen to not incorporate physical token use, as it is not feasible to have websites with millions of users send out unique physical keys to each and every user on their website.

We have either mandatory or optional two-factor and two-step authentication as the differentiation allows for two clearly different user experiences. Mandatory two-step authentication would require a lot more effort from users, which some would consider too much work. Optional two-step authentication would give users who are looking for additional security the option for it, while also not inconveniencing less diligent users.

Email verification would come in the form of an email with a token that is sent to a user's email address when they first log in. This email token should be clicked on in order to allow the user access to their newly created account. Ideally, users should re-verify their email address once every year, to make sure that an email account has not yet been recycled. If a user cannot verify their address they should be able to choose a new address to use for that website.

When a website has restricted access, users who have not yet verified their email addresses should not be able to make full use of the website's services. The website itself should decide which restriction would be in place.

4.3 Decision Tree

Finally, when we combine all the variables and actions mentioned above, we can rank them in terms of importance. With this we have obtained the following decision tree:

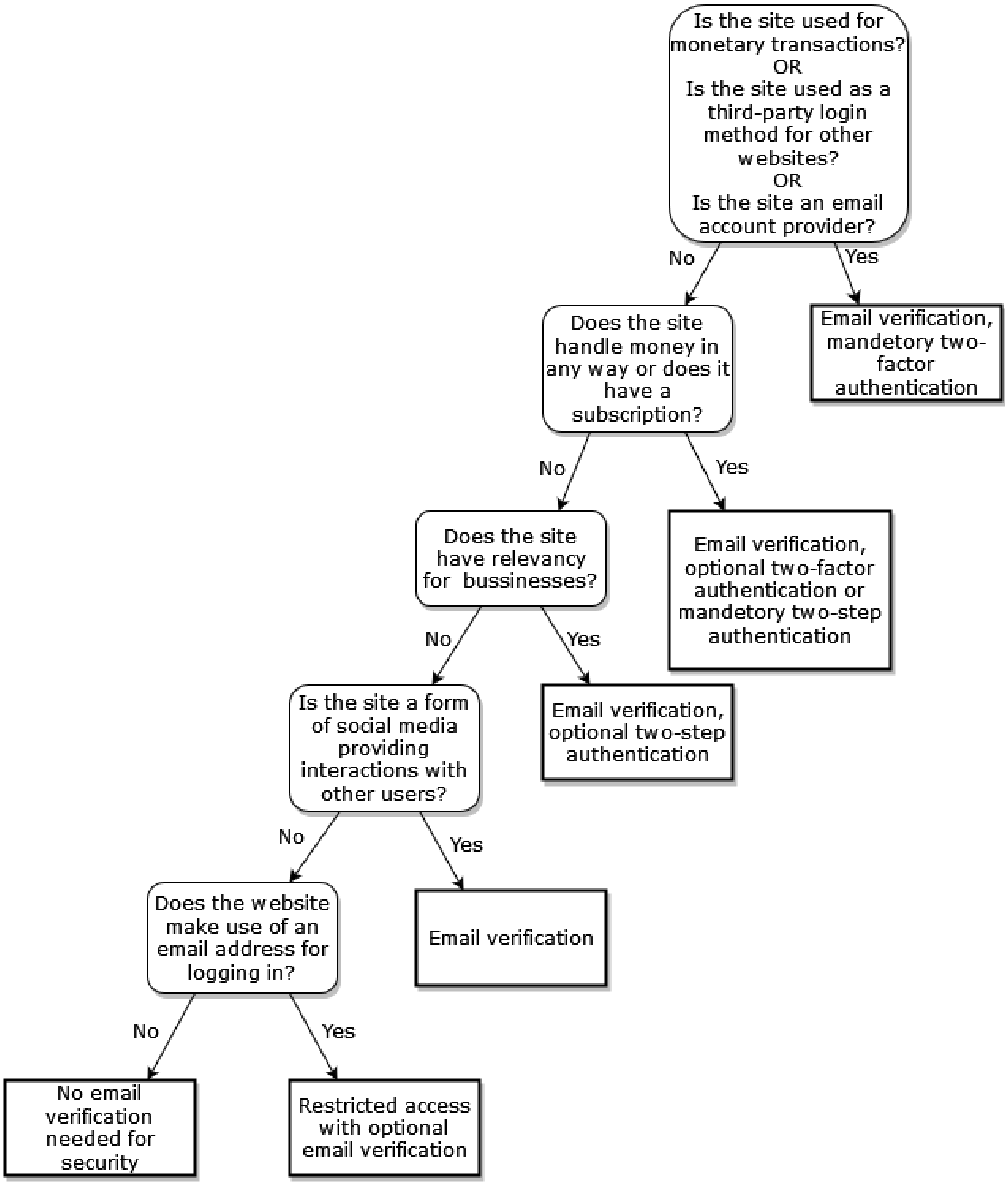
Is the site used for monetary transactions? OR Is the site used as a third-party login method for other websites? OR Is the site an email account provider?
No
Yes
Does the site handle money in any way or does it have a subscription?
Email verification, mandetory two-factor authentication
No
Yes
Does the site have relevancy for bussinesses?
Email verification, optional two-factor authentication or mandetory two-step authentication
No
Yes
Is the site a form of social media providing interactions with other users?
Email verification, optional two-step authentication
No
Yes
Does the website make use of an email address for logging in?
Email verification
No
Yes
No email verification needed for security
Restricted access with optional email verification

Figure 4.1: The resulting decision tree

4.3.1 Examples

Let us take Google as an example for the decision tree. Firstly, we know that Google is used as a third-party login method for many other sites as well as them being an email service provider, we also know that they offer users with the Google Pay services, which handles transactions on some websites. Because of this we would stop at the first leaf of the tree, meaning Google should make use of email verification and mandatory two factor authentication, which is the case.

Another example would be Marktplaats. This is a website that doesn't directly make monetary transactions for users, but does handle money by allowing users to make purchases. Additionally, they do not provide third-party login options to other websites. This means that Marktplaats should at least use email verification and either mandatory two-step or optional two-factor authentication. Marktplaats does make use of mandatory two factor authentication and email verification, which is a level of security above what is expected. This does however by no means imply that they should downgrade their security.

Chapter 5

Related work

So far, there has not been a lot of research done on this particular subject, as most studies related to emails are more oriented towards the subjects of spam and phishing. Phishing is common because of a multitude of reasons, and while some users are more susceptible to such attacks, awareness is an important factor. This means that emails greatest issue next to spam problem can be reduced through increasing awareness. [3] Phishing can furthermore also be solved relatively efficiently though the use of machine learning. This is would most likely also work for regular spam. [1] This makes unverified and recycled email addresses a serious problem due to other issues having a more obvious solution.

We believe that unverified and recycled email addresses are relevant not only because of the importance of email addresses in of themselves [6], but also for the integrity of user accounts on other websites. They are commonly used, despite being older technology and still having some issues. They are easy to create at a variety of websites, while also providing access to many other websites due to them being used as login credentials. [7]

Likewise, email addresses are still crucial when two-factor and two-step authentication is used, as many websites include email addresses in their authentication process. Two-factor authentication using smart phones can still be bypassed using clever attacks. [2] [8] Additionally, two-factor authentication won't defend against phishing and password loss, as identity theft will still occur. [9]

Resetting passwords through emails is easily exploitable through all kinds of attacks, including social engineering and additional (mobile) hardware exploitation. [10] Man-in-the-middle attacks can also be used when a user resets their password. This works on popular sites like Google and Facebook where two-factor authentication could still be exploited, but email verification and stricter measure may help reduce this risk. [11]

Finally, email-based identification and authentication is an emerging alternative to public-key infrastructure. [12] This type of research would be supported by adding security to email addresses on all websites.

Chapter 6

Conclusion

Unverified and recycled email addresses are a security risk for user accounts on many different types of websites. We have analysed many popular websites that have various levels of security regarding email addresses and two factor authentication. A significant number of them allow users to use unverified and recycled email addresses in order to create an account, which leads to the risks of users losing that account.

Luckily, this risk can be mostly mitigated through a combination of two-factor authentication, two-step authentication and most importantly email verification. None of these methods are completely foolproof, but they greatly increase the difficulty of performing attacks that can result in the takeover of an email account. We have analysed the level of security each website should have and have combined the above mitigations into a decision tree. Websites can use this decision tree for choosing the right set of policies for them. With this, websites would mitigate attacks in most cases and thus protect their user's accounts from being stolen.

Bibliography

[1] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," in *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, (New York, NY, USA), p. 649–656, Association for Computing Machinery, 2007.

[2] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, "On the (in) security of mobile two-factor authentication," in *International Conference on Financial Cryptography and Data Security*, pp. 365–383, Springer, 2014.

[3] J. Wang, T. Herath, R. Chen, A. Vishwanath, and H. R. Rao, "Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email," *IEEE Transactions on Professional Communication*, vol. 55, no. 4, pp. 345–362, 2012.

[4] A. Holmes, "533 million facebook users' phone numbers and personal data have been leaked online," 2021.

[5] N. Routley, "Ranking the top 100 websites in the world," 2019.

[6] M. Afergan and R. Beverly, "The state of the email address," *SIGCOMM Comput. Commun. Rev.*, vol. 35, p. 29–36, jan 2005.

[7] V. Kumar, K. S. Vaisla, and J. Kishore, "Analyzing email account creation: Expectations vs reality," in *2014 Fourth International Conference on Communication Systems and Network Technologies*, pp. 597–600, 2014.

[8] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[9] B. Schneier, "Two-factor authentication: too little, too late," *Communications of the ACM*, vol. 48, no. 4, p. 136, 2005.

[10] C. Routh, B. DeCrescenzo, and S. Roy, "Attacks and vulnerability analysis of e-mail as a password reset point," in *2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ)*, pp. 1–5, 2018.

[11] N. Gelernter, S. Kalma, B. Magnezi, and H. Porcilan, "The password reset mitm attack," in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 251–267, 2017.

[12] S. Garfinkel, "Email-based identification and authentication: an alternative to pki?," *IEEE Security Privacy*, vol. 1, no. 6, pp. 20–26, 2003.