Crypto | Seb

Account Takeover via Mobile Compromise

Draft: August 5th, 2020

Joshua Johnson (CryptoSeb)
W: https://cryptoseb.pw
E: root@cryptoseb.pw
Keys: .pw/keys

Introduction:

Hello wonderful people of CAMEL, Joshua here. I guess now you get to see my alias that I have used in the privacy/security community for many years. I go by the handle CryptoSeb but many just call me Seb. There's no relation to my real identity, I just had a very small child named Seb sitting on my lap when I made my Twitter. I'm going to do my best to describe the shenanigans that has happened with one of our members over the last few days, but am still wrapping my own head around much of it, so I will likely need to update this document as my own contacts in the area become available to help me compile information and resources for you all and edit what I already have.

I'm certainly not an expert of any sort and won't ever claim to be. These are just my thoughts and suggestions. Some of them could be wrong (hands up emoji here, but it's better than nothing, right?

Backstory:

On Monday, August 3rd, 2020 a member of our community here was hit with an identity attack that basically turned her day upside down. This attack is one that has become increasingly popular over the last 5 (or so) years, but not one many of you are likely to have heard of. So, from what I can tell, this individual was a victim of what's known as a "SIM Swap Attack", which could also be known as a port-out attack (this method is a bit different than what she experienced) or SIM Jacking. I'll explain more on this later.

When this individual woke up in the morning, she didn't have any cell service. She recounts that this felt odd, but that she had WiFi and so continued about her morning as usual. Later that morning, she realized something more was going on and found out that her phone seemed to be "disconnected". She then found out that she had lost control over her Email account (Hotmail / Microsoft) and attempts were made to access her PayPal. The attack seemed to stop here, and I was then in touch to help her regain accounts and work to thwart further compromise. She got a new SIM activated in her phone, but still doesn't have details from her phone company on how this attack was played out.

What happened?

Honestly, I'm not entirely sure. My money is on a SIM Jacking Attack, but we're still trying to determine whether that's the case or not. To give you a bit of explanation, a SIM Jacking Attack works by having an attacker get the contents of the SIM card that's currently in your phone transferred out electronically to another SIM that they own (in

their own phone). This means that phone calls, text messages, voicemails, and account details are now registered to their SIM. They retain your phone number, but it is now registered to their own phone. You're probably asking how attackers can do this without your consent, and the explanation is rather simple: customer support typically sucks. People can often "trick" Customer Support over the phone (or sometimes in person) to do what they want. Go watch these two videos now:

1. https://www.youtube.com/watch?v=fHhNWAKw0bY

2. https://www.youtube.com/watch?v=PWVN3Rq4gzw

So, what can we do about this?

This is one of the many aspects that I'm still in the process of fine-tuning and figuring out. The issue is that many of the more secure solutions simply do not work for the average, or more tech-illiterate user. For it to have been a 24hr long personal adventure, running thought circles in my mind basically all night yesterday, it's evidently not just a "click here and be done" problem. Nor is it a problem that can be solved in ways the average user will be competent enough to do on their own (not to shoot any of you down here, but being honest about our strengths and weaknesses is a good thing).

The major flaw in the way we authenticate for our accounts online is that it has largely been dominated by email + password for the last 20+ years. The insecurity with this is that users will, more often than not, reuse passwords across websites and expose their email to the general public. A recent shift over the last 5 or so years has been to authenticate with a user's phone number, at least when it comes to password resets. This could be seen as a bit of an improvement for the average user because we are now moving forward into an age where your cell phone is almost always on your person. When you can't login to your account, you can just receive a temporary access code via text/call to change your password. Or when a website doesn't recognize your login, it, again, can just send you a text message for confirmation.

Because almost all of our online identity is tied to either our email, or our phone (in some way or another), an attacker just needs to compromise those two vectors and they can gain access to almost anything else in your name. And I hate to be the bearer of bad news, but your email is probably secured with a password + your phone number as a recovery option. So again, if they gain access to your mobility account, they gain access to everything.

Let's dive a bit deeper, shall we?

In this CAMEL individual's case, she was using a Hotmail account, which is run by Microsoft. Once her phone was compromised, the individual went straight for her primary email account. From here, they reset her password and changed the recovery information on her account, effectively locking her out of her account. One of the things they DIDN'T do (thankfully) was logout of all other sessions on her email. This would have meant that she didn't receive any of the updates on her phone's email inbox at all. Microsoft's automated systems thankfully caught onto this as an attack/compromise and locked her account for 30 days. She can't receive emails or change key parts of her email until this 30-day period is up, so that's a pain in the ass.

There's two primary ways that this sort of attack can be thwarted (I think, maybe):

1. Your mobile number is not tied to your online accounts

2. The provider for that account/website/service employs additional security measures on top of just requesting a code that is sent to your phone.

Unfortunately, #1 isn't as easy as one might think. And #2 isn't a widely adopted practice yet. Companies want to make things as convenient for their users as possible. If they are met with challenging "setup" pages for a new website/service, users are likely to say screw it, and leave to find something else. So, there's now a balance between security and convenience that often leaves the user's account open to compromise because the company chose the latter in their design.

What I would recommend:

First and foremost, we need to understand that this form of attack isn't the only way someone can compromise your identity online. There's still a plethora of attacks happening daily that play on individuals using weak passwords or reusing the same few passwords across multiple websites. Your first "goal" is going to be to move away from a password model that requires YOU to remember them. When you're tasked with remembering a different password for every site you register on, it's near impossible. BUT, if you only have to remember 3 or 4 really good passwords, that's not such a daunting task.

Step 1: You need a password manager (or a safe way to store them)

A password manager is crucial in maintaining one's safety online, in my opinion. The idea behind them is that a user is far more equipped to keep their individual accounts secure if they only have to remember one password. Password managers do this by creating a "vault" where users store their online identities, website login information, and other important articles of their online life. These vaults are typically end-to-end encrypted (this means the data you store in them isn't readable by anyone who doesn't know the password) and deployed with strong security practices that actively work to keep your accounts safe. It can be difficult for an individual to begin using a Password Manager, but the learning curve is manageable with some attention towards understanding how it works and then setting it up to fit your needs. I personally have used LastPass and currently use Bitwarden to manage my online life.

What Bitwarden usage looks like:

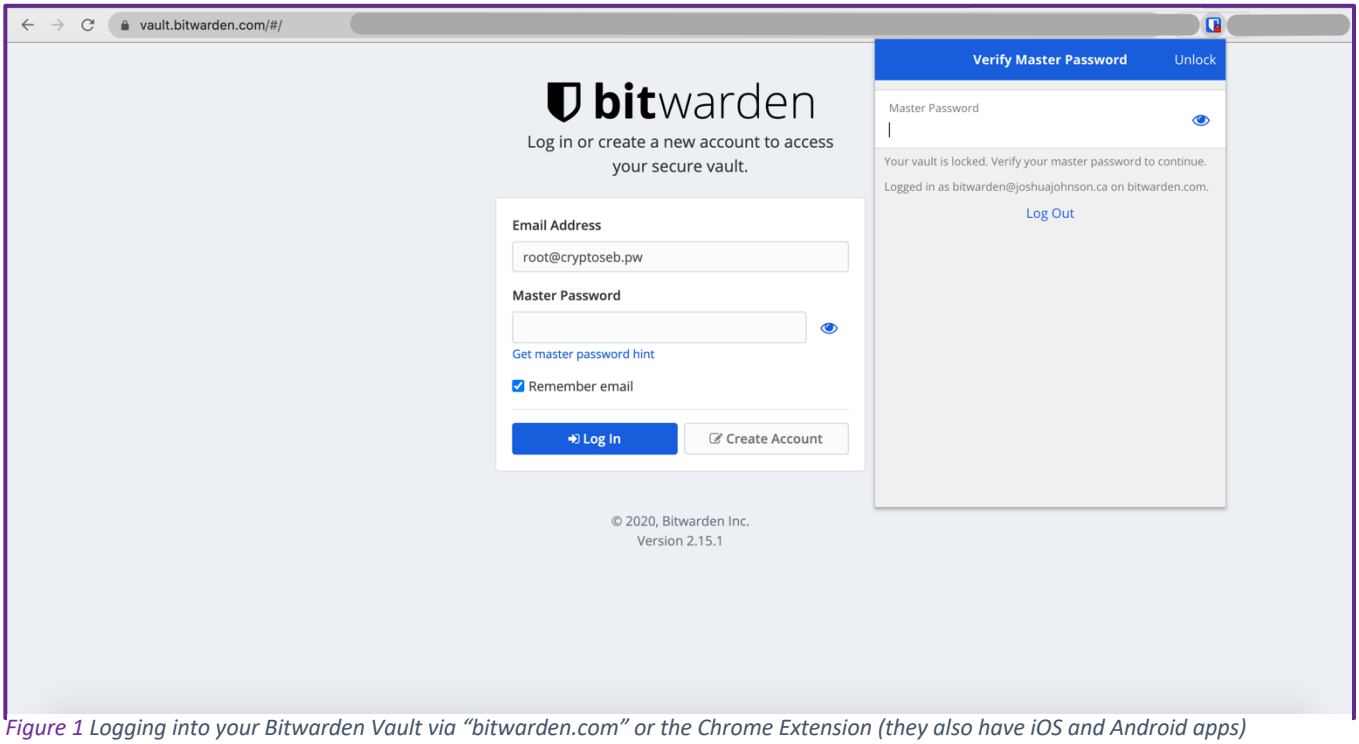

Figure 1 Logging into your Bitwarden Vault via "bitwarden.com" or the Chrome Extension (they also have iOS and Android apps)

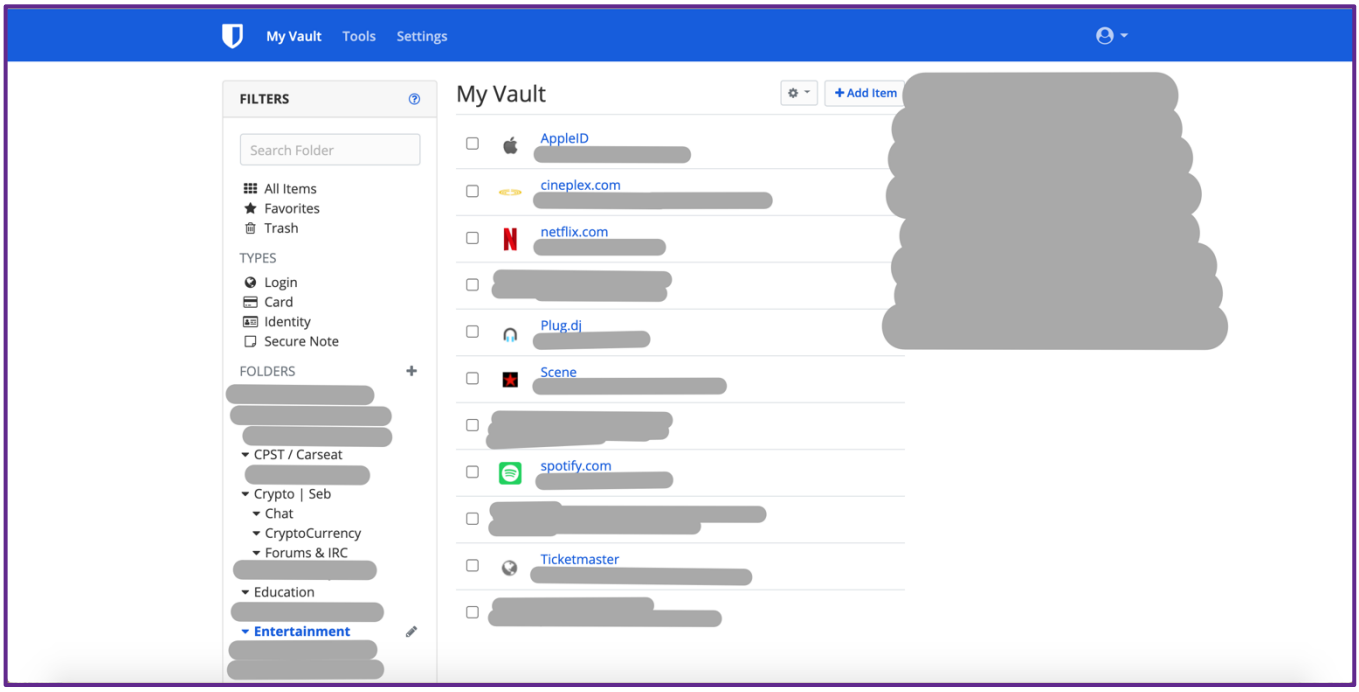

Figure 2 What my vault looks like when I open it. I can organize everything into folders for easy access

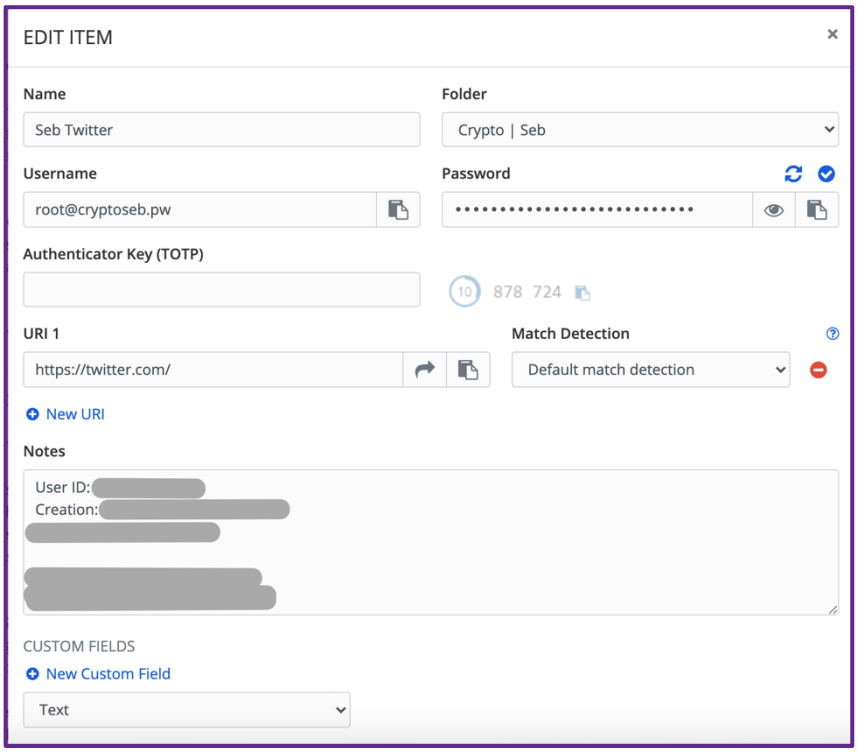

Figure 3 Viewing login information for one of my "Twitter" accounts. I can add any relevant information for this account in the Notes section. I could also upload files (like a screenshot of recovery codes), etc.

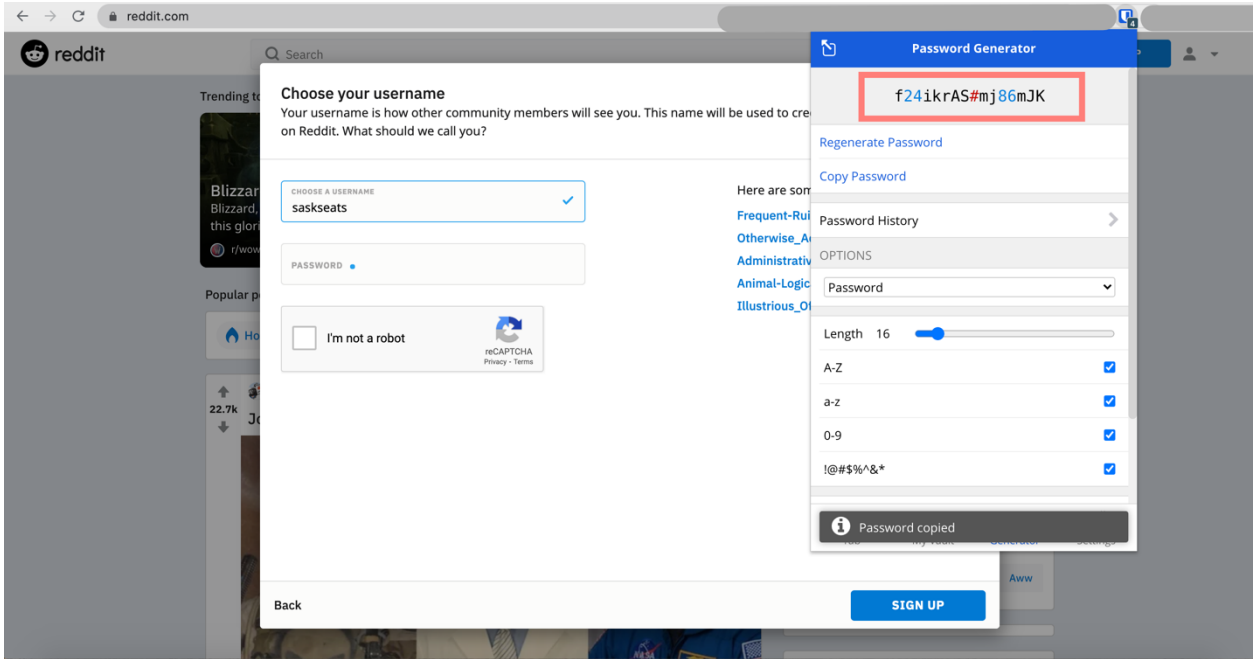

Figure 4 Creating a Reddit Account is super easy. Here I am having Bitwarden generate a random password for me. I put that into the password field on Reddit and click to sign up.

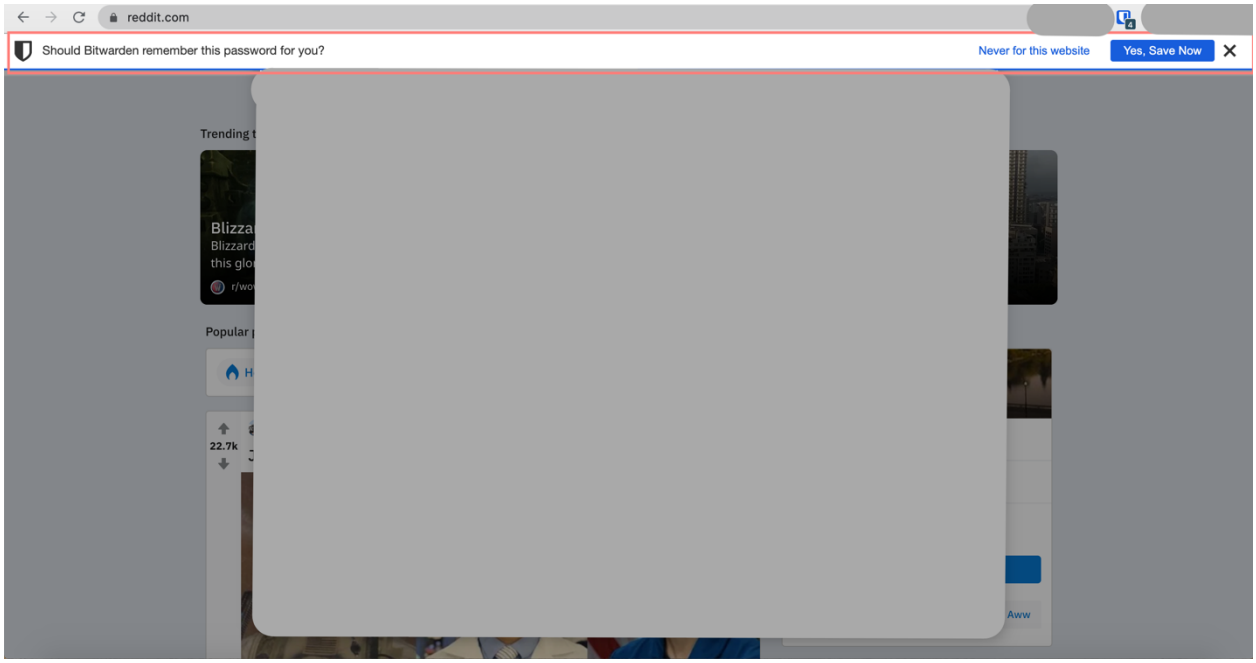

Figure 5 Now Bitwarden asks me if I want to save the password in my vault. We'd click "Yes, Save Now"

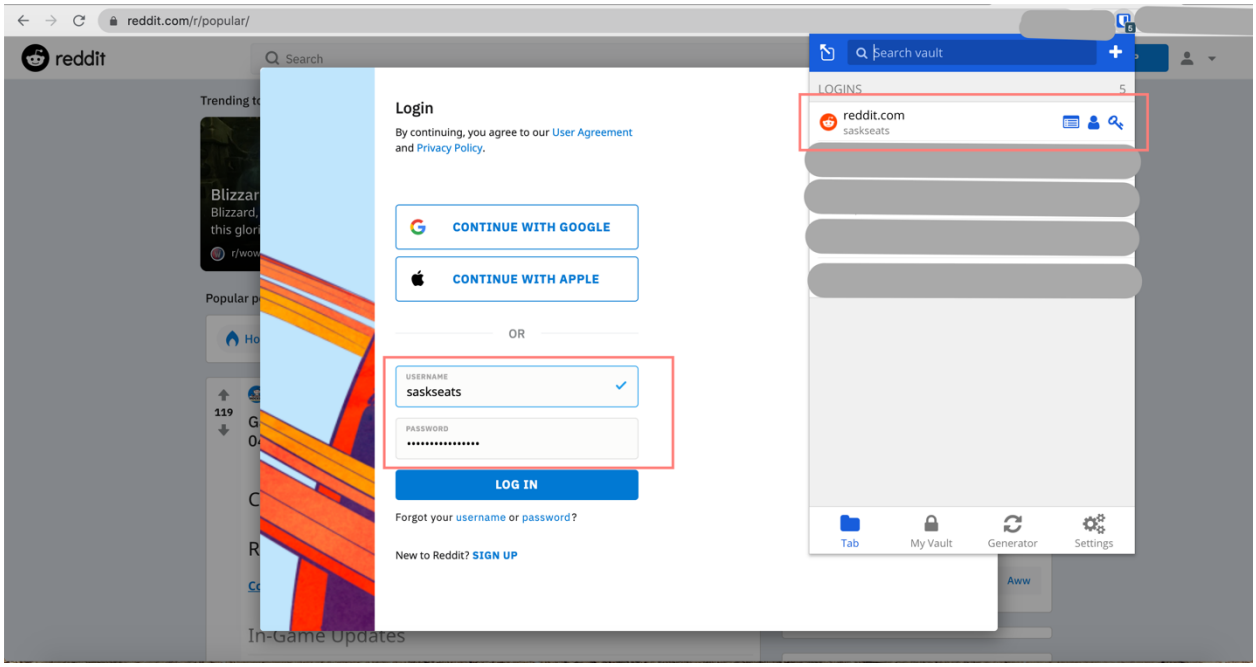

Figure 6 Now I can login to Reddit.com with my new account by visiting the website (or loading the app on my phone), clicking the Bitwarden Extension, and selecting the Reddit account I want. It will autofill the username and password it just saved.

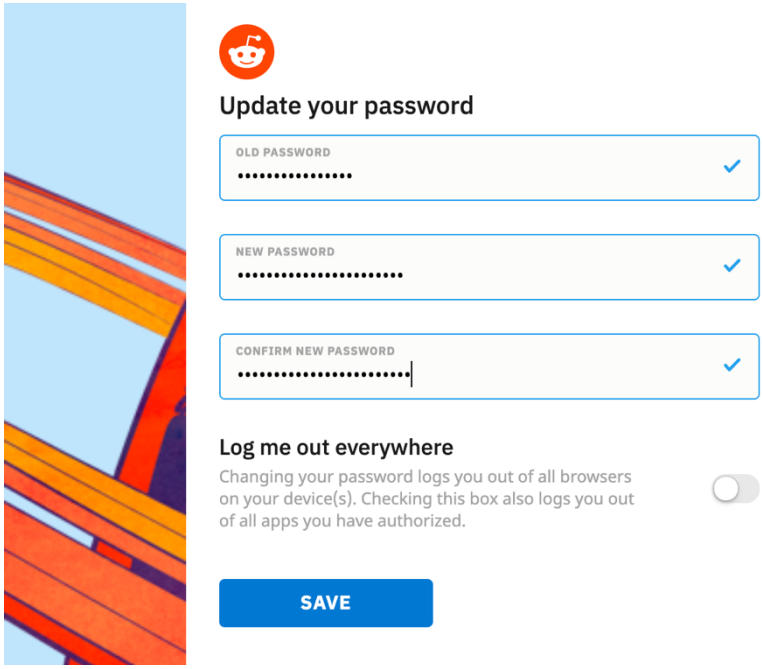

Figure 7 Need to update an account? No problem. Just go change that account password and let Bitwarden handle the rest.

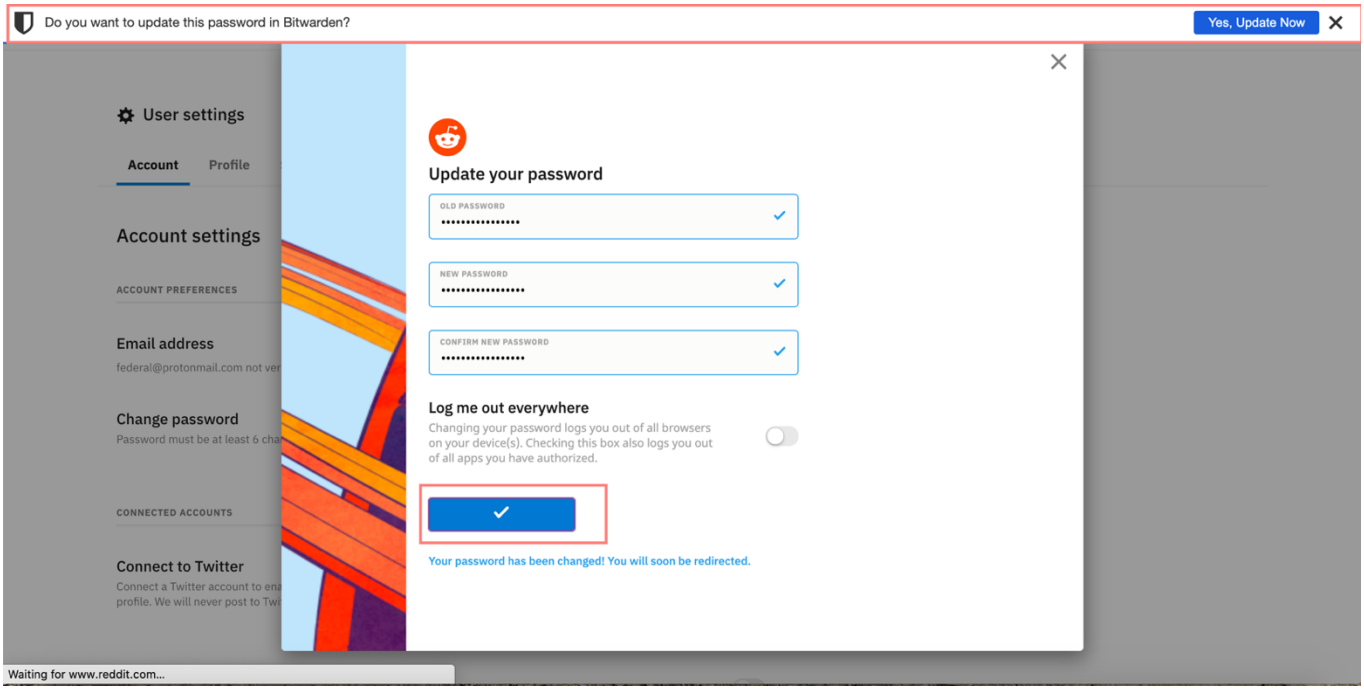

Figure 8 Bitwarden asks me if I want to update the password in my vault. I click yes. It's that easy.

Step 2: Make sure your email is "as secure as it can be"

Although one would assume all email is created equally, it isn't. It's also pretty hard to determine what makes a good email provider in this specific case, because some providers that have wonderful security/privacy practices shit the bed when it comes to features. So, I'm not going to discuss which providers to avoid (but clearly after seeing Microshit lock our friend out of her account for 30 days, I probably won't endorse them here), but can say that I personally use ProtonMail and Google/Gmail. ProtonMail is my daily driver and is linked with a few of my domains. It's an encrypted email provider based out of Switzerland (shameless plug here, they are f*cking awesome). Google is used for other things like my Calendar and YouTube, but I rarely actually use the Gmail part of that account.

After Monday's adventure, I would recommend NOT linking your phone to your email account as a method of recovering your account. Instead, we'd ideally have two-factor authentication set up (discussed more in a bit) and link it to a secondary email account that we are using for recovery. Although not fool-proof, few providers actually require more than just one factor of authentication to reset a password. You'll read on about how Firefox does a wonderful job at password resets though.

Step 3: We need hardware or software token Two-Factor Authentication (TOTP / 2FA)

As mentioned in my previous paragraphs, there really isn't a perfect system for password recovery. We want to be notified when a potential breach happens on our account, but don't really want the "recovery" system to only require one step. Ideally, we'd have to go through a few steps to regain control, all the while being notified that this is happening.

Strong Two-Factor Authentication can help us here though, because it means you need something more than just a password to login. Ideally, if they reset your password, they still need this "other thing". TOTP (Time-based one-time password algorithm) is based on the idea that "something you have" is generally better than "something you know". But unlike your mobile number being used as "something you have", TOTP is cryptographically secure, and isn't constant. The science behind this uses time mixed with a secret key for each account you setup TOTP with. The result is an app like Authy (my personal favourite), or Google Authenticator that generates codes required to login. The website knows the codes, because of math and complex algorithms. Authy knows the codes, because of math and compl… anyways, let me show some examples with pictures again.

What Authy usage looks like:

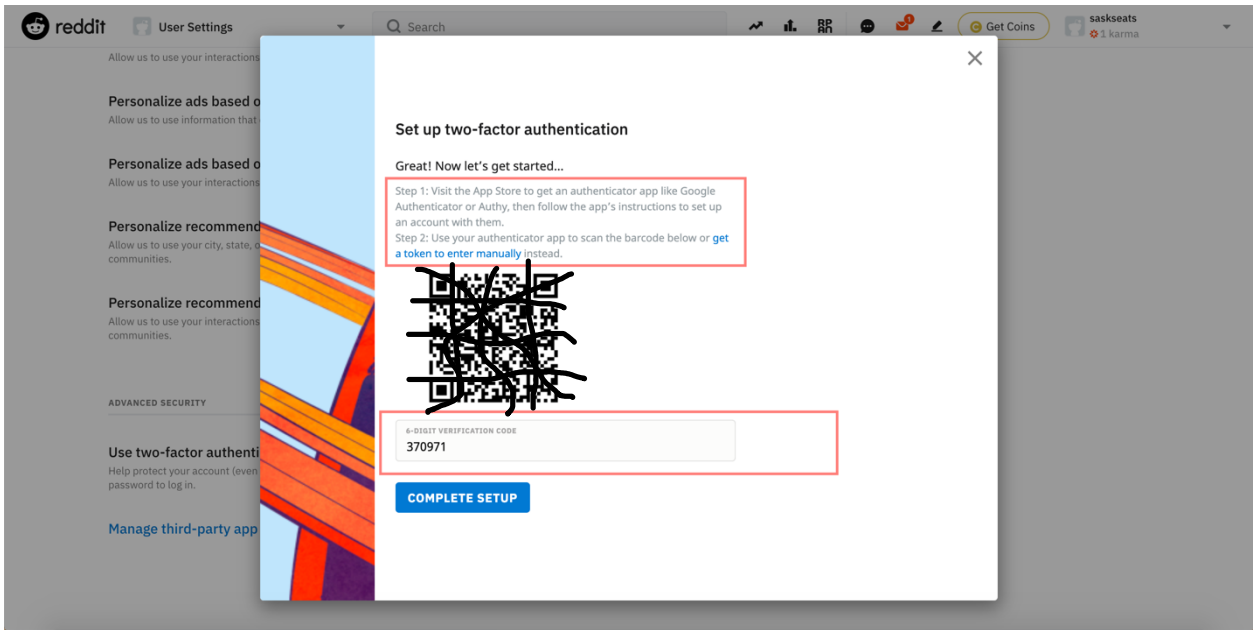

Figure 1 Enabling TOTP is simple with Authy. You just use Authy to scan the QR code (or copy/paste the secret key) and then paste the code it generates back into the website.

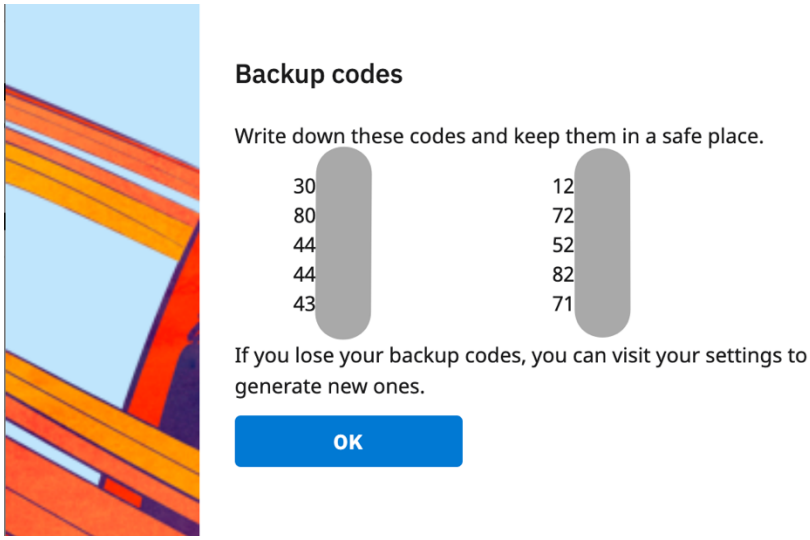

Figure 2 It also generates backup codes incase you lose access to Authy (you could store these in Bitwarden, or print them and put the paper in your filing cabinet)

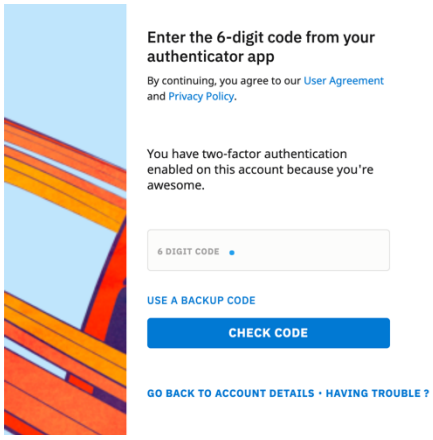

Figure 3 When I go to login, I put in my username and password and then it asks for one of these codes. The codes change every 30 seconds in the Authy app (remember, it's not constant like a phone number).

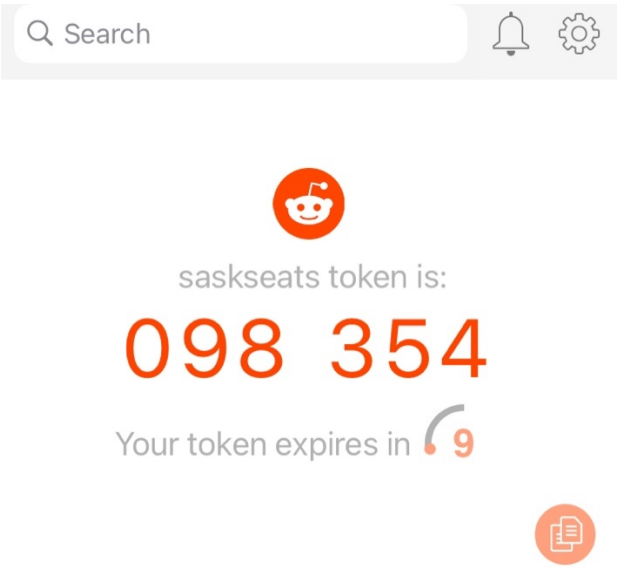

Figure 4 This is what Authy shows when I search for my Reddit account. I would type this code in to the input field on Reddit and click check code to login. If it hadn't expired, Reddit would log me in. This whole process adds like 30 seconds MAX to each login to a site once you get familiar with it.

Note: The reason I like Authy so much is because it allows me to backup my authentication codes on their server in an encrypted format. This is useful in case I ever lose my phone in a toilet, or some toddler angry pitches it into a wall at work. But this is also why websites will often generate backup codes for you; they too understand that toddlers can be assholes and you don't want to completely lose access.

Step 4: Call your mobile phone provider & other companies

When you call them, you can ask to enable "Port Protection" for your account. This will prevent someone, or at least make it harder for them, from porting your number out to a new provider. This won't prevent a SIM Jacking Attack, but it will certainly help (at least my phone provider tech dude seemed to think so). You can also ask them what steps they take in terms of password recovery or how they would handle a SIM swapping attempt. The guy on the other end of my call said that he's well aware people may try to social engineer him on the phone, which is why they have a very strict policy on requiring two pieces of identity confirmation. This policy is "fair", but neither of the two things he required are perfect. I'm fairly confident it would thwart an attacker who didn't know much about me though. I'd be more pleased if they required me to login to my mobility account and had a specific section where it would generate a support key for the customer service rep on the phone to authenticate a SIM swap/number port. Even better, just don't do it over the phone. It's that easy.

Step 5: Consider what avenues companies go down for password recovery

As discussed above, many providers don't require much more than a code sent to your email or phone. This isn't good, because if either one of those recovery options is compromised (we've proven this is doable), it's very easy to hijack that account. Things like security questions aren't overly secure either because they are:

a) Easily guessed when people make them commonly known facts
b) Aren't typically hashed on the company's server (hashing refers turning something into a scrambled representation of itself), so they can be leaked in a company data breach
c) Forgotten by the user or mistyped at creation. I once wrote "taco" instead of "tacos" as my Favourite Food and got locked out for a solid week from a forum.

But if you have to use security questions, consider putting a symbol behind your dog's name, so as to obscure the process for an attacker. "Rex" becomes "Rex$", "Disney" becomes "Disney$", you get the idea.

I won't go into "what" companies should be doing for password recovery, but you can read more here: https://duo.com/decipher/reality-of-online-account-recovery Duo put some of the big names to the test back a few years ago.

Wait, I just said I wouldn't go into this, and here I am. In my defense, I typed this out for a different section and moved it. Here's some of the companies I went through the "Account Recovery" features for:

PayPal – it was brutal. I was able to reset my password with my phone AND reset my TOTP authentication with my phone. So… both forms of authentication were reset because I had a mobile number linked to my account. Support said the only way around this is to link a landline to your account instead (which I did). Considering they handle large sums of money and have important pieces of my identity on file, I expect better.

Google – I was able to reset with my phone (SMS, Phone Call, Gmail App) or recovery email (it sends a code). This would NOT disable TOTP and I would need to input a backup code or fill out a support form to disable that. Pretty good. I still removed my phone from the account though, just to be safe. I have the Gmail app on my phone, and it notifies me of all sign in attempts.

RBC – They don't support TOTP 2FA, which is really sad. But they do support Personal Verification Questions and you can set it up to ask you one every time you login (highly recommended). I was able to bypass this feature, but I called support and addressed it.

It will be getting patched. Their phone support uses "Secure Voice" to authenticate your voice when you call, and they representative doesn't need to verify any details with you as long as your voice matches the voice file they have for you. Password reset is via SMS, which is also bad, but there's no way around that unless you unlink your phone from their system, which means they can't call you to notify you of fraud they have detected on your account. I opted to leave my phone number attached. I think it's more important that my bank has it to contact me in an emergency, than it being used maliciously in a password reset (maybe that's backwards thinking).

Amazon – Sends a code to your email. I'd say this is more secure than sending to your phone in many cases. This doesn't bypass TOTP, but I can get a code texted to my phone as a backup (kinda shitty). I wasn't able to figure out a way to disable this, but at least my phone isn't being used for both reset features? That's good?

Facebook – I removed my phone, so the only way to receive my recovery code is via the email attached to my account. I have PGP encrypted emails set up, which adds a big second layer of security, but it's a very complicated that you don't need to worry about. If this method failed, I could also use my trusted contacts. Facebook is typically pretty good at this, but I did have a friend get locked out of his account for 2 weeks last year. He had to scan a picture of his Passport AND send them proof of his residence to get back in. Proving that, apparently, Facebook knows where you live?

Snapchat – Could reset with either my phone or email, but I had to input either of them in order to do so. It likely recognized my iPhone and didn't require an OTP from Authy. I like that it wanted me to input them, and didn't even give me the dumb r*****@cr****.pw bullshit. We all know my email is root@cryptoseb.pw, I list it publicly. You'd be affording me far more security by not listing anything at all.

Firefox – Arguably the best out of the above. It had me create a "Recovery Key" (xxx xxx xxx xxx xxx) when I created my account and I setup TOTP authentication with Authy as a second step of login security. When I went to reset my password, it first emailed me a link to click. I clicked the link and it asked for the recovery key I had generated when my account was created. If I didn't put it in, it would wipe stored passwords, history, bookmarks, etc. before proceeding. Then it took me to a page where I had to create a new password. Finally, it asked me to put in an OTP code from Authy. I got an email every step of the way too, so my phone would have been blowing up (in the incredibly minute chance someone was able to go through these steps to take my account).

Final remarks, I suppose

As you can probably see from the 15 pages of (hopefully not so gibberish) content, securing your identity online isn't super easy. Hackers and account thieves put in arguably more work to find ways to take our accounts than the majority of us do to protect those accounts. But there is proof (like this video that Marc shared: https://youtu.be/uyf0eOkuxYA) that these individuals can turn your life literally upside down and backwards in a matter of hours. Even scarier, Michael Terpin lost over $20 million dollars in Bitcoin (an online currency) back in January of 2018 due to a SIM Swap/Jacking attack. Another individual lost his entire retirement savings when his investments were hit after a SIM Swap/Jacking attack. But people don't just go after those with considerable money either, they'll take what they can get. So, if you're on the bottom of the security totem pole, you could be a pretty big target.

This is another good blog about the topic, minus the Authy being hacked party, because that's not true (you just need to enable "authenticated encrypted backups" in the Authy Settings and specify a good password). Funny how he neglects to mention this.

https://www.thewolfofallstreets.io/security-tips-and-lessons-learned-from-my-hack/

That's all for now folks,

Seb / Joshua
August, 2020

To contact me regarding this document, you can get in touch with me via the listed methods on my website, or through email if you have to. Initial messages through Facebook are fine, but I'd like to move all in-depth conversations over to Signal or other reasonably secure chat applications (like Element, or Keybase Chat, or even WhatsApp).