

Security Training



Part 1: Technical Setup

This purpose of this section is to install and configure your laptop with all of the necessary applications to get started working at ShapeShift



Passwords at ShapeShift

- You only need to memorize TWO passwords
 1. Your laptop password
 2. Your 1Password master password
- **Every** other password is stored in 1Password



Methods for Memorizable Passwords

Hard:

- Password → Memory



Easy:

- Memory → Password



Methods:

1. Bruce Schneier's Method
2. The Mind Palace Technique



Bruce Schneier's Method

- Take a sentence and turn it into a password.
 - Should be **personal** or **memorable** to you
 - Abbreviate words and combine them in unique ways to form a password

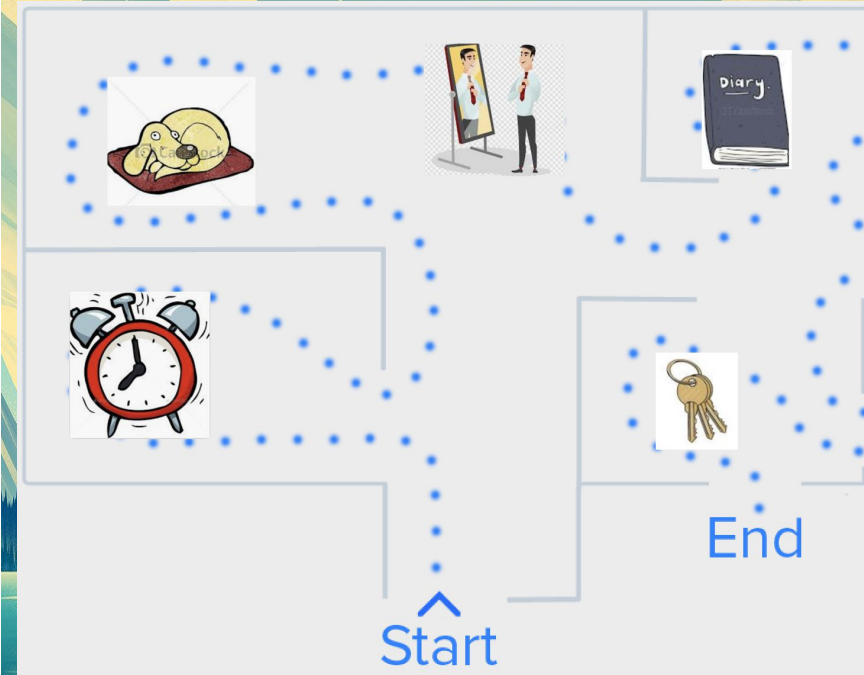
Examples:

- W00!TBwontSB
 - Woohoo! The Broncos won the Super Bowl!
- Ilf,w/asCooP/na()
 - I like fruit, with a scoop or in a hoop.



Technique to turn an existing memory into a strong passphrase

1. Pick an existing place and time from memory (i.e. childhood bedroom)
2. "Look around" the room. What do you see?
 - (clock, dog bed, mirror, diary, key)
3. String those things together to form the password
 - Add some numbers and/or symbols
 - 1Clock,Dogbed,mirror.Diary.keys
4. **NEVER USE THINGS YOU CAN LOOK UP**
 - It must be a **PERSONAL** memory





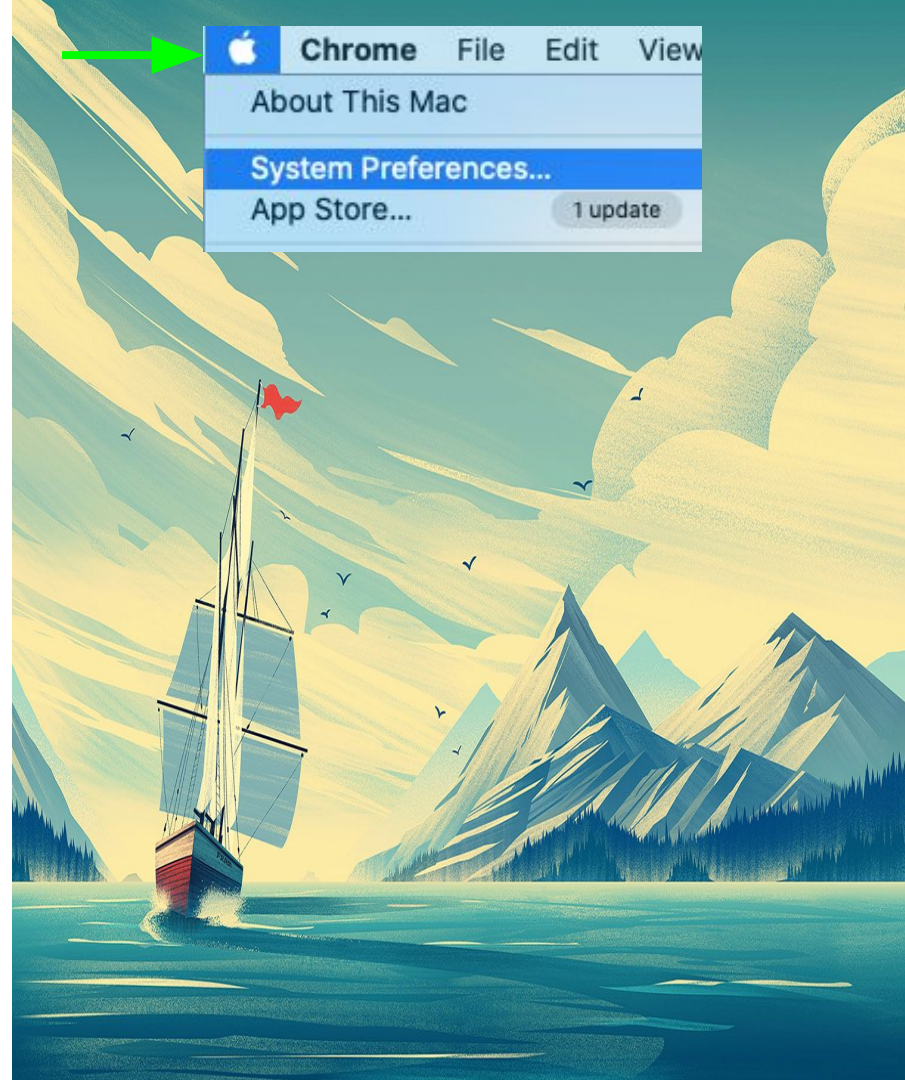
Do what's best for you!

As long as you can memorize the password easily

Laptop Password

To change your laptop password:

- Go to System preferences → Users & Groups → Change password
- Password policy (section 5.2)
 - **Must** be unique for every account
 - **Must** be a minimum of **14** characters
 - **Must** contain mixed case
 - **Must** contain numerals
 - **Must** contain non alphanumeric symbols



Install a Supported Browser

Safari doesn't support all Yubikey functions.

Choose a browser that does:



Chrome (<https://www.google.com/chrome/>)



Firefox (<https://www.mozilla.org/en-US/firefox/new/>)



Brave (<https://brave.com/download/>)



Opera (<https://www.opera.com/download>)

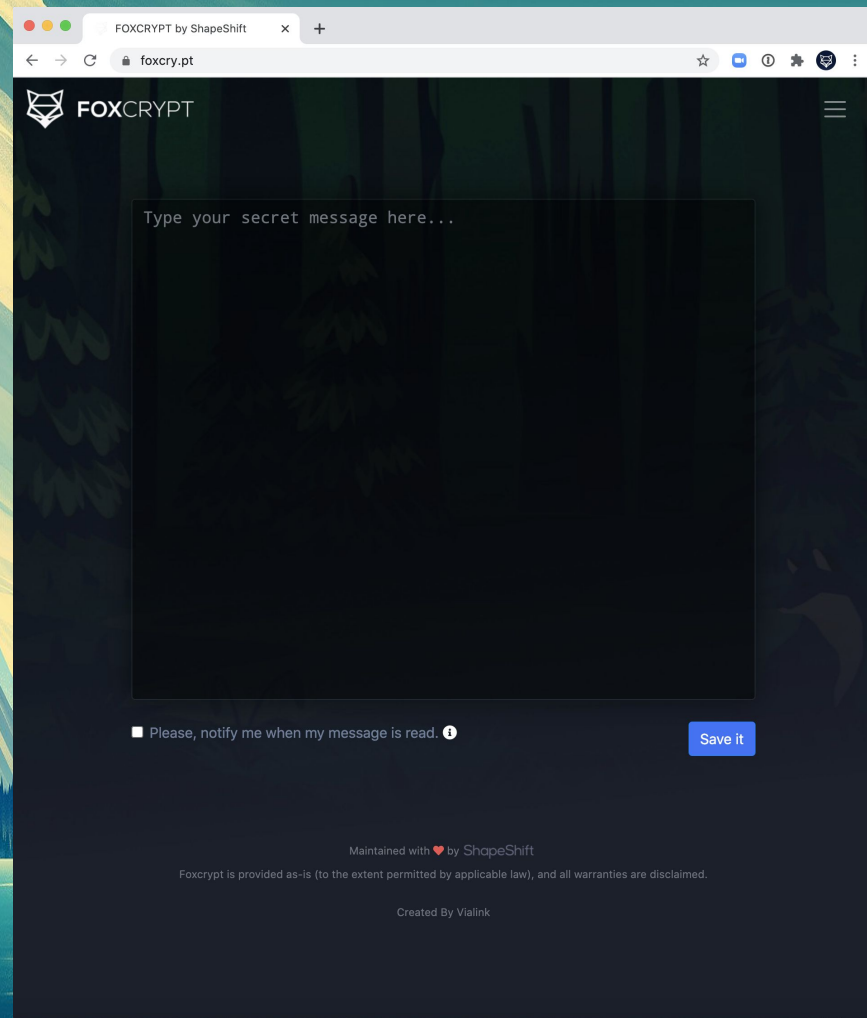


foxcry.pt

Website to quickly and securely share text with others (<https://foxcry.pt>)

- Auto-destructs messages after they're read
- Great way to share API keys, temporary passwords, and other sensitive data with foxes

Bookmark this tool in your favourite browser now



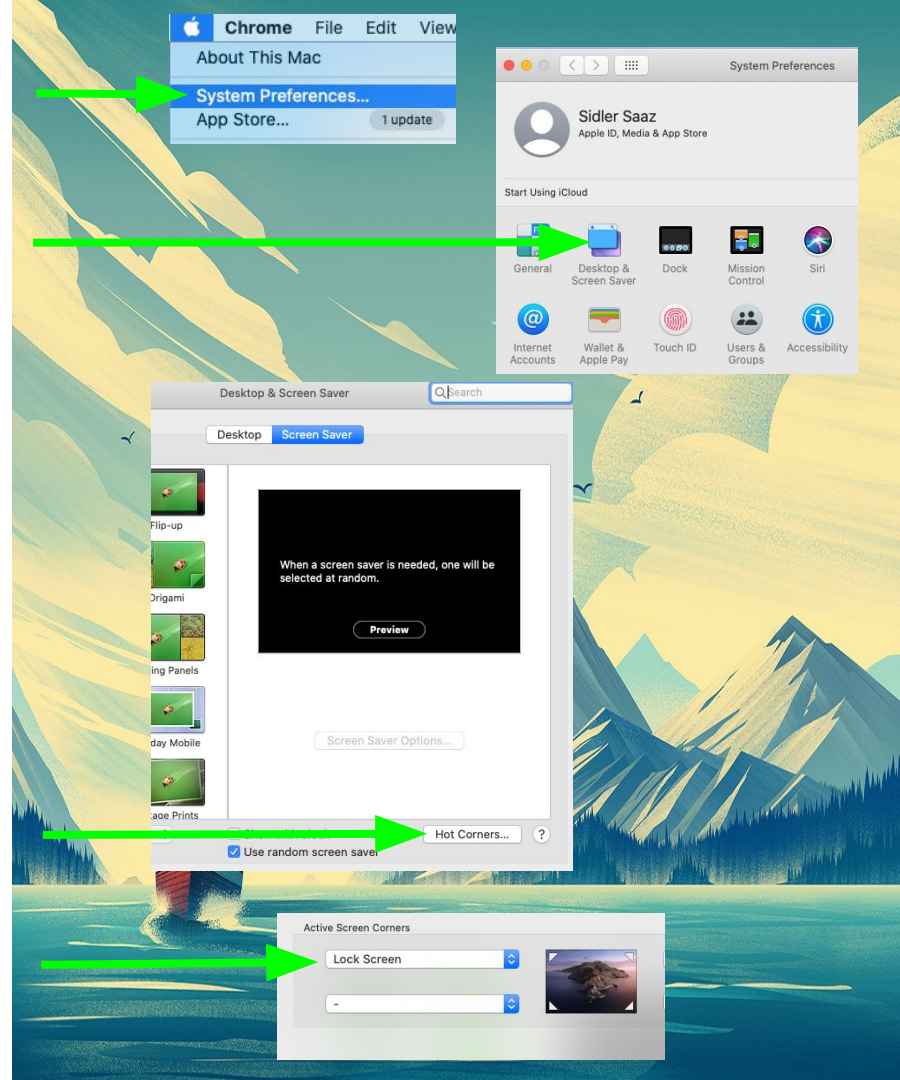
Lock Your Laptop

- You must build the habit of always locking your laptop when you're away from your computer
- Default lock time 10 mins (mdm policy)
- With Mouse: Apple menu → Lock Screen
- With Keyboard: Ctrl+Cmd+Q
- You may wish to configure a Hot Corner too



Lock Your Laptop

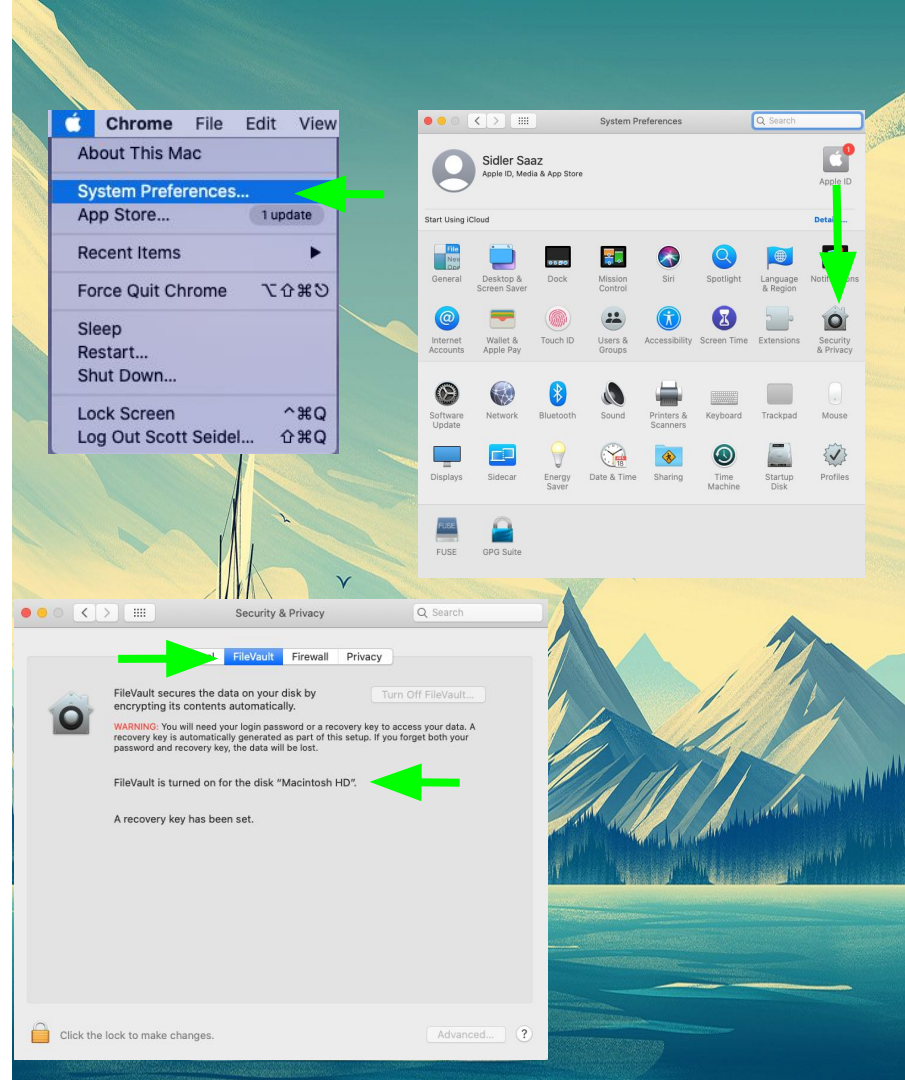
- Another method for quickly locking your screen is to set up a Hot Corner (optional)
- Go to System Preferences → Desktop & Screen Saver
- Click Hot Corners
- Pick a corner and choose the Lock Screen option



Check FileVault


FileVault encrypts the entire contents of your hard drive so if your laptop is lost or stolen the data is safe.

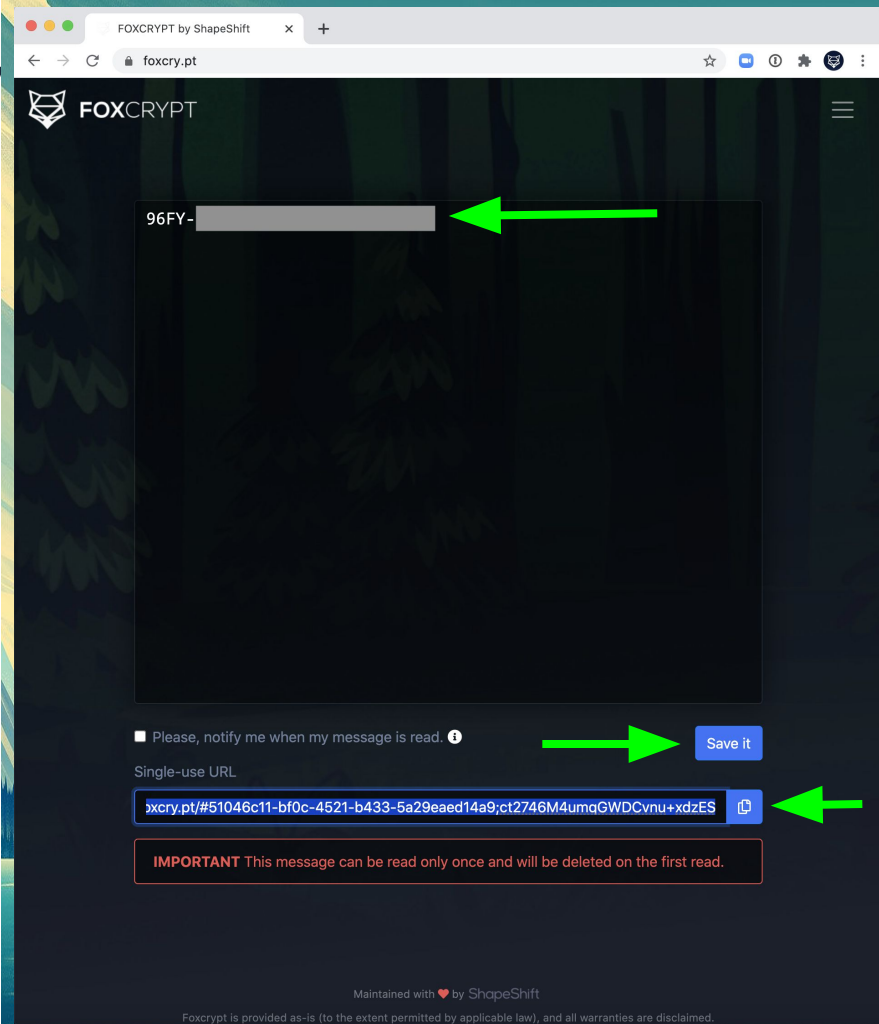
- Make sure FileVault is enabled
 - Apple menu → System Preferences → FileVault → FileVault is turned on for this disk “Macintosh HD”
- If it's not enabled, ask Security/IT to assist



Send FileVault Recovery Key

Send the FileVault recovery key via foxcrypt.

- Go to website (<https://foxcry.pt>)
- Copy the FileVault Recovery Key from open terminal window and paste it in foxcry.pt
- Click 
- Copy the URL & Paste the URL in a direct message to a member of the security team



1Password

Why do we use 1Password?

- A safe & encrypted place to store passwords
- Easy to share them if needed
- Easy to generate unique random password for all accounts
- Avoids bad password habits



1Password Setup

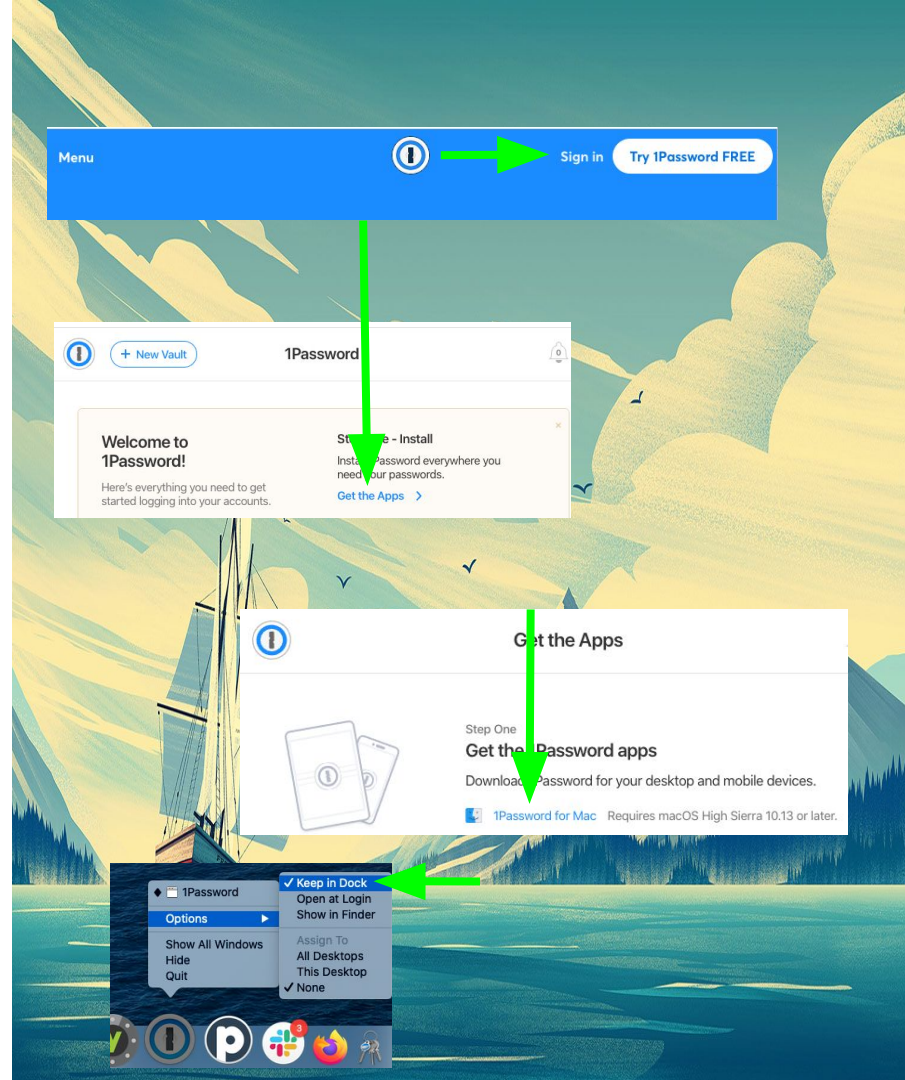
1. Login to your Alias gmail inbox
2. Accept invite for 1Password
3. Choose a Master Password
 - Remember tips for how to make memorable passwords!
4. Print and store emergency kit offline
 - **Delete the digital copy after printing**
 - **Do not keep a digital copy!**



1Password App

Install the Application:

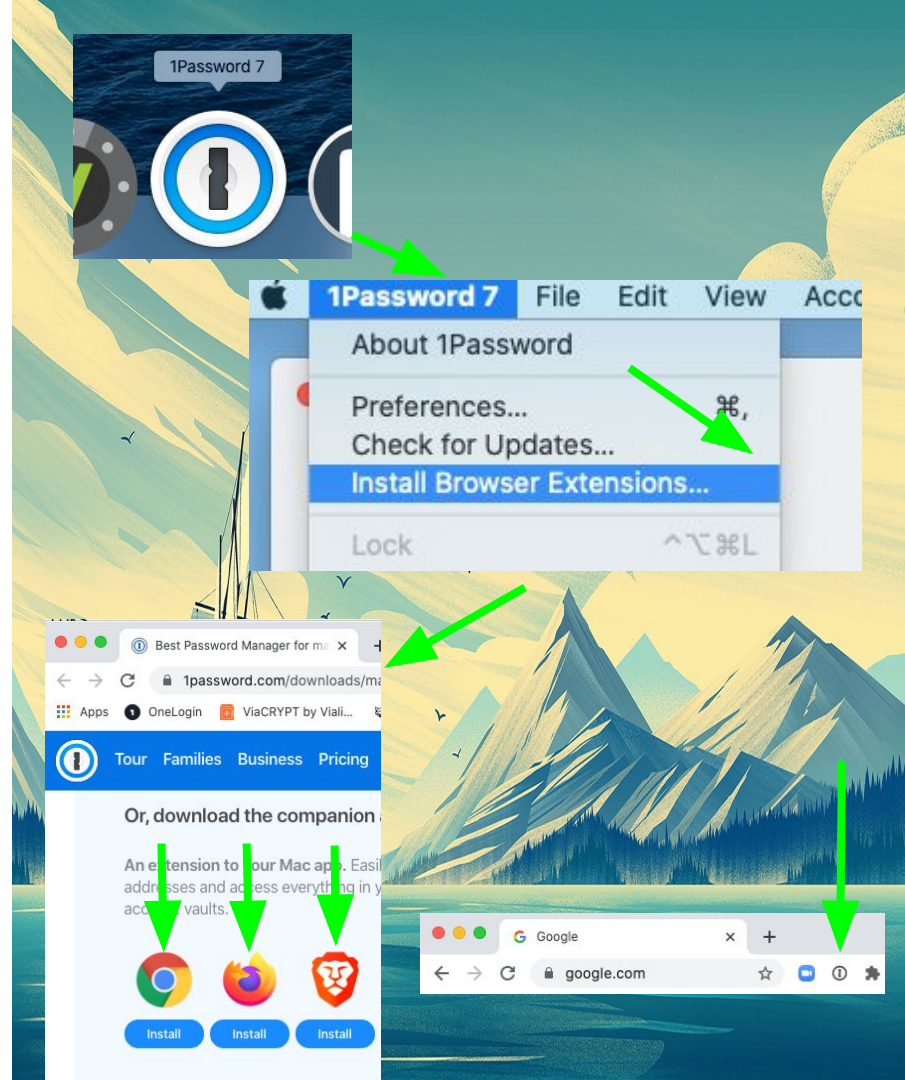
- Login to 1password.com (<https://1password.com/>)
- Click on [Get the Apps](#)
- Click on [1Password for Mac](#)
- Recommended:
 - Select the option to “Keep in Dock”



Install 1Password Browser Extension(s)

Installing the Browser Extension(s) :

- Launch the 1Password Application
- Go to the 1Password menu → Install Browser Extensions
- Select the installer for the browser(s) you have installed
- Extension should now show in your browser(s)

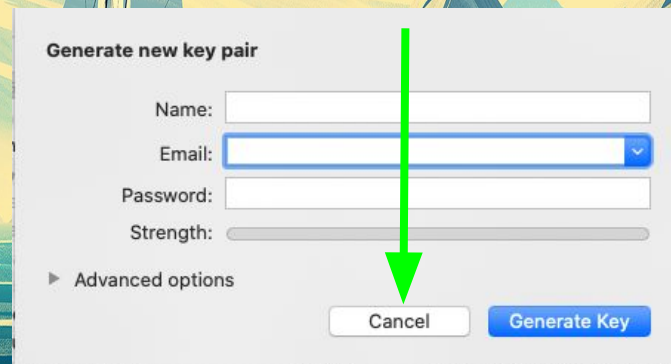
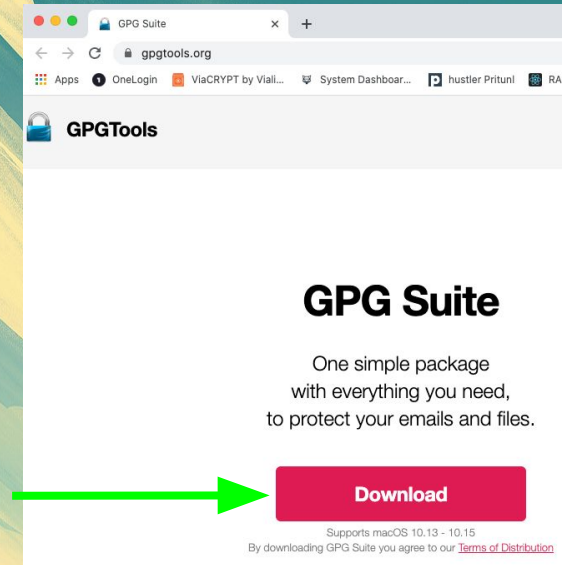


GPGTools

- GPGTools is used to encrypt, decrypt, sign and verify files or messages.
- This allows you to detect impersonation

Install GPG Tools (<https://gpgtools.org/>)

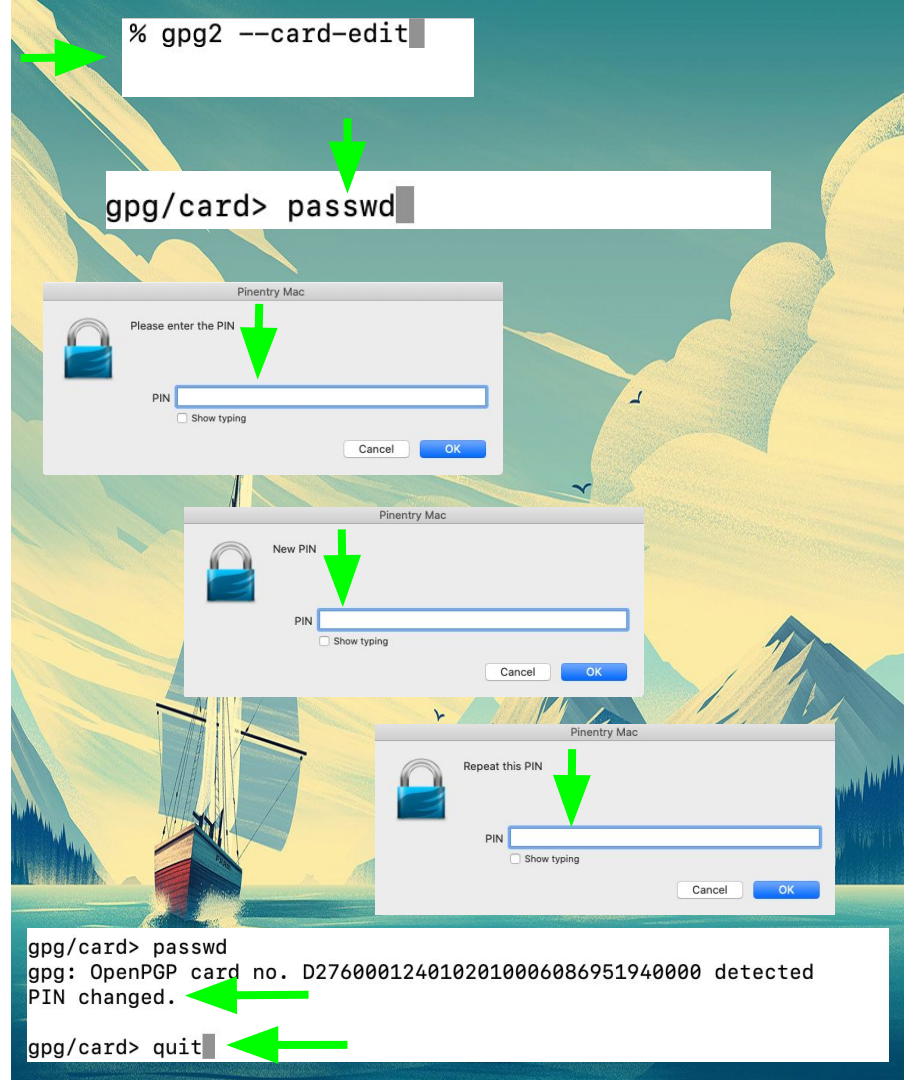
- Download and install the .dmg image
- Click **Cancel** when prompted to generate a new key pair
- Your key pair has already been generated
 - Yubikey (private key)
 - Pubkeys.zip (all ShapeShift public keys)



Set Your GPG PIN

Setup your personal GPG PIN:

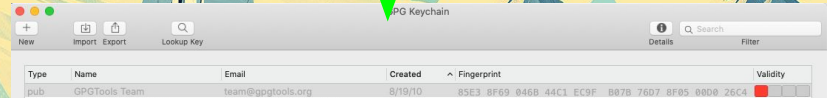
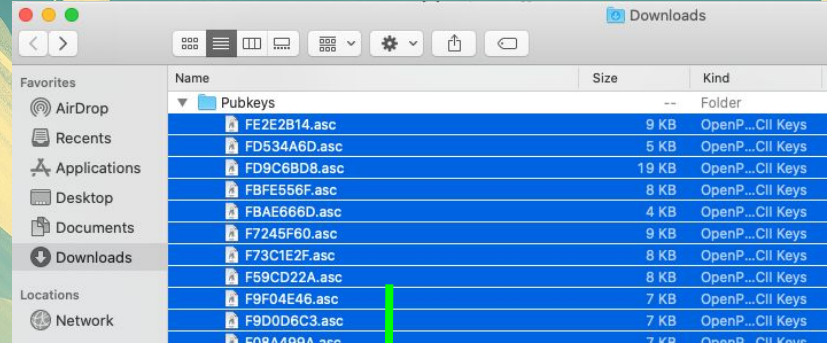
- Create a new 6 digit PIN in 1Password
 - Name it "Yubikey PIN"
- Change your Yubikey's PIN
 - Insert your Yubikey
 - Open "Terminal"
 - Type: `gpg2 --card-edit`
 - Type: `passwd`
 - Enter the default PIN (security provided)
 - Enter your new PIN and verify



Install Employee Public Keys

Add all employee public keys to your GPG keyring:

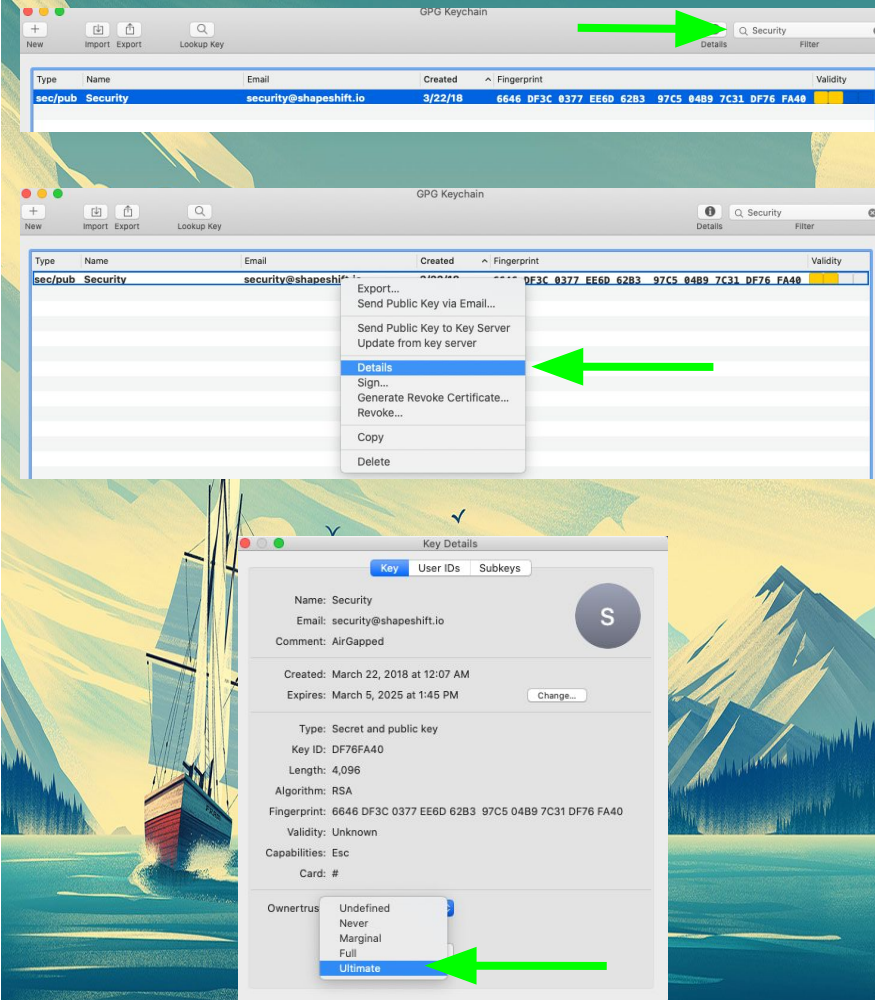
- Download Pubkeys.zip from <REDACTED>
 - Unzip into a temporary folder
- Open GPG Keychain app
- Select all the keys and drag them into GPG Keychain



Trust "Security" Public Key

Trust the "Security Public key:

- Open GPG Keychain app
- Search for security@shapeshift.io
 - Make sure the fingerprint matches:
6646 DF3C 0377 EE6D 62B3
97C5 04B9 7C31 DF76 FA40
- Highlight the Security Key
- Right Click and go to Details
- Ownertrust → Ultimate



Yubico Authenticator

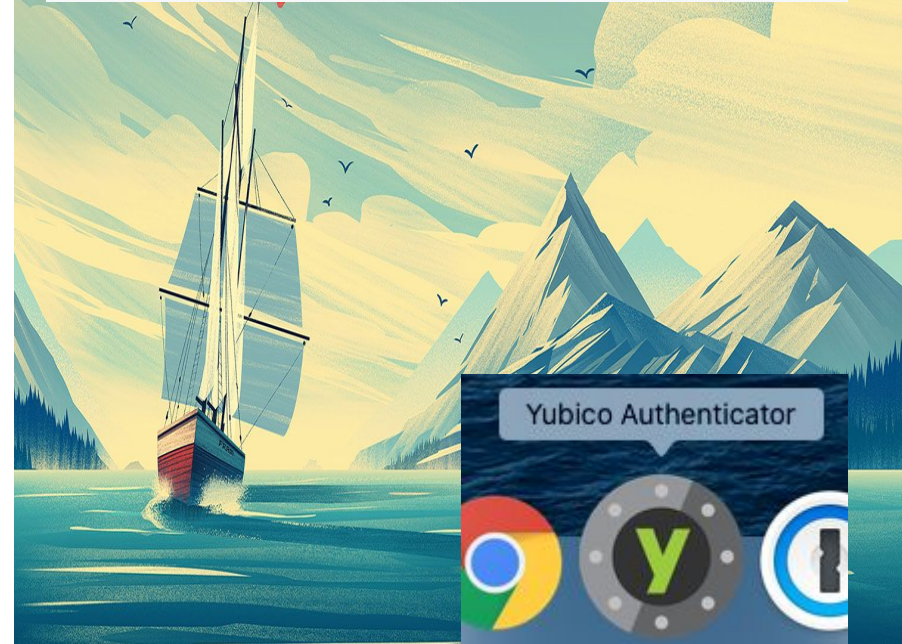
Yubico Authenticator is an app that helps keep your ShapeShift accounts secure.

- Works like Google Authenticator, but uses your Yubikey
- Install Yubico Authenticator:
 - Download the installer (<https://www.yubico.com/products/services-software/download/yubico-authenticator/>)
 - Run the installer
- Recommended:
 - Keep Yubico Authenticator pinned in your Dock




Desktop Yubico Authenticator

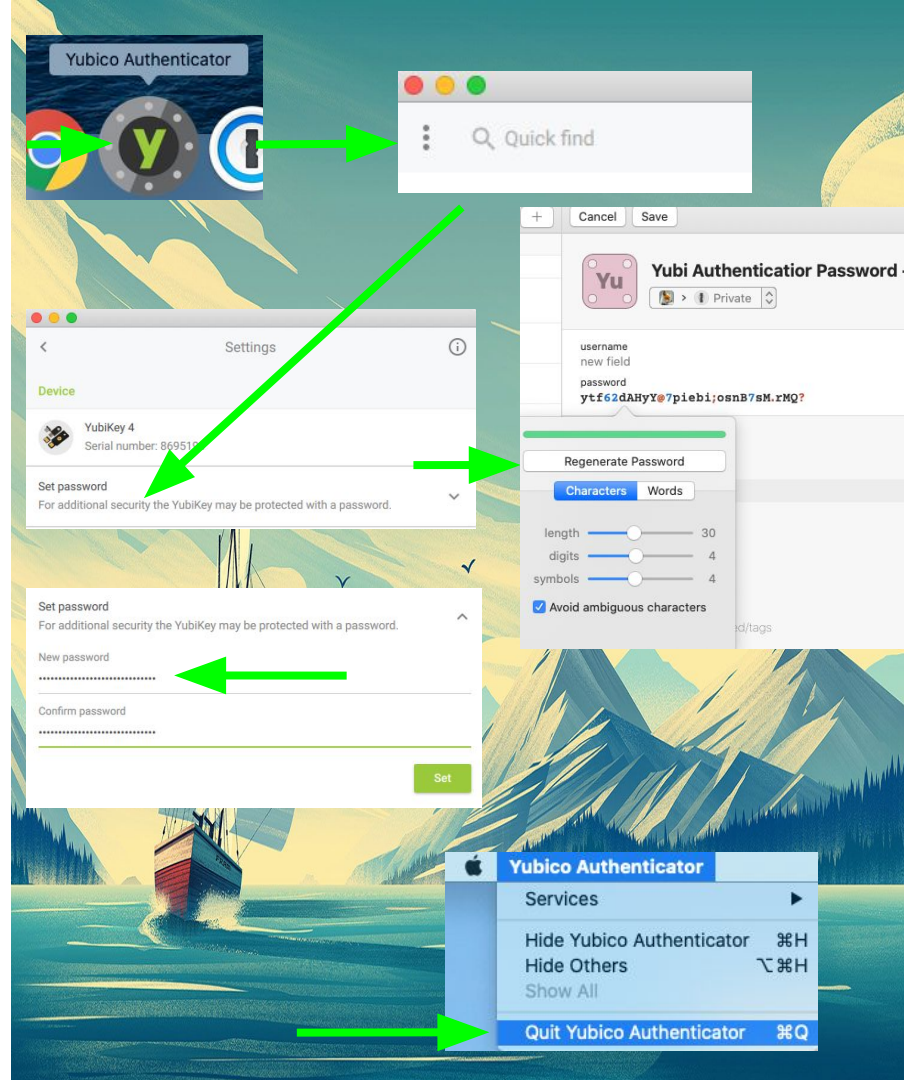
Use the Yubico Authenticator for Desktop on your Windows, Mac, or Linux computers to generate OATH credentials on your YubiKeys.

- Linux Download
- Mac (OS X and macOS) Download
- Microsoft Windows (32 Bit) Download
- Microsoft Windows (64 Bit) Download



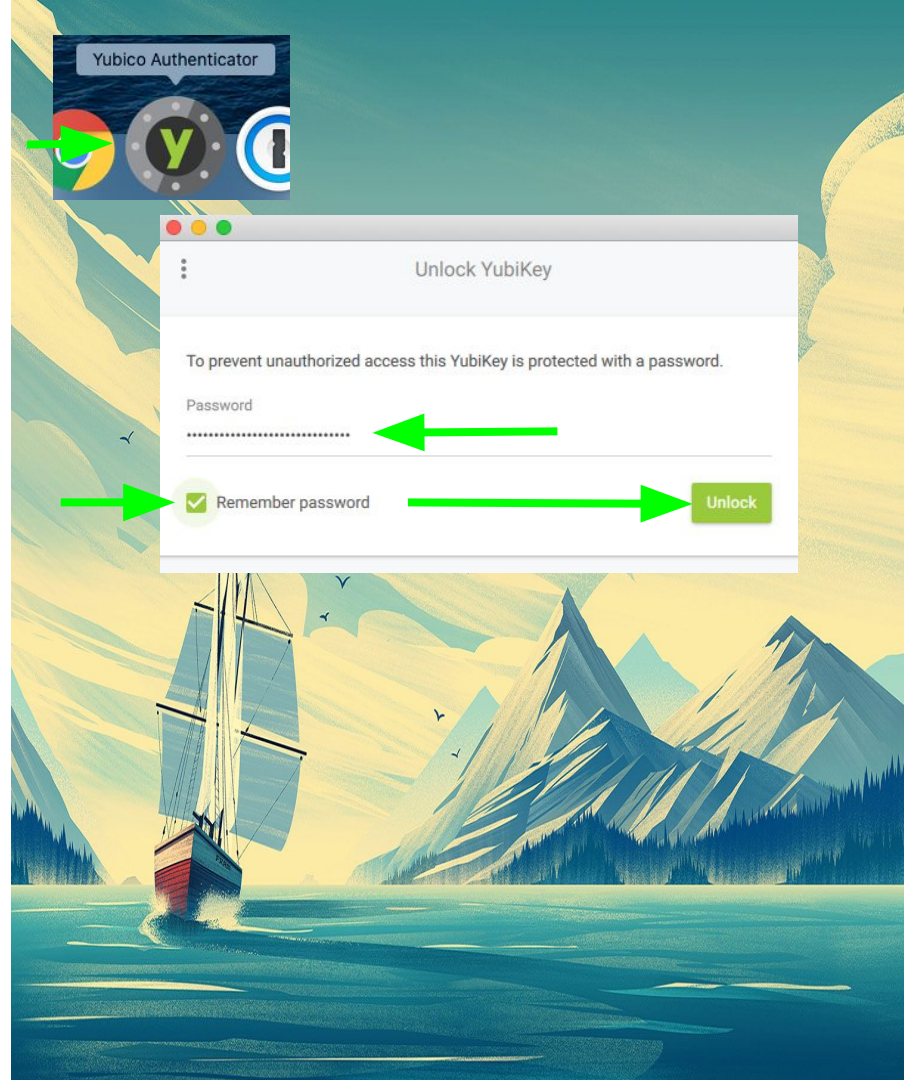
Add a password to Yubico Authenticator

- Create a new password
 - Open 1Password 
 - Create a new password record
 - Name: Yubico Authenticator
 - Save it
- Insert your YubiKey
- Launch Yubico Authenticator
- Click on Settings (3 dots) 
- Click on **Set Password**
- Copy your Yubico Authenticator password into the *New Password* textbox
- Click 
- Quit Yubico Authenticator



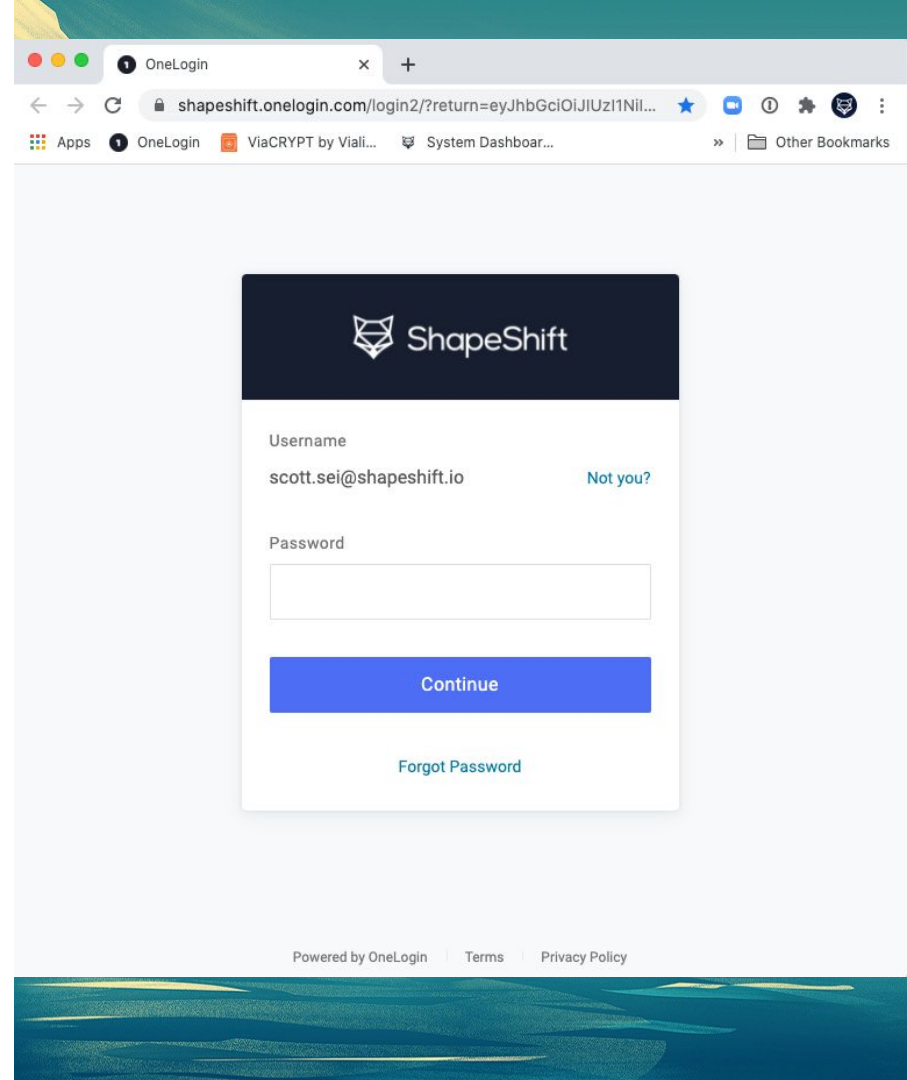
Save Yubico Authenticator Password

- Insert your Yubikey
- Launch Yubico Authenticator
- Enter your password from 1Password
- ☒ Remember password
- Click
- Restart Yubico Authenticator to verify it is saved



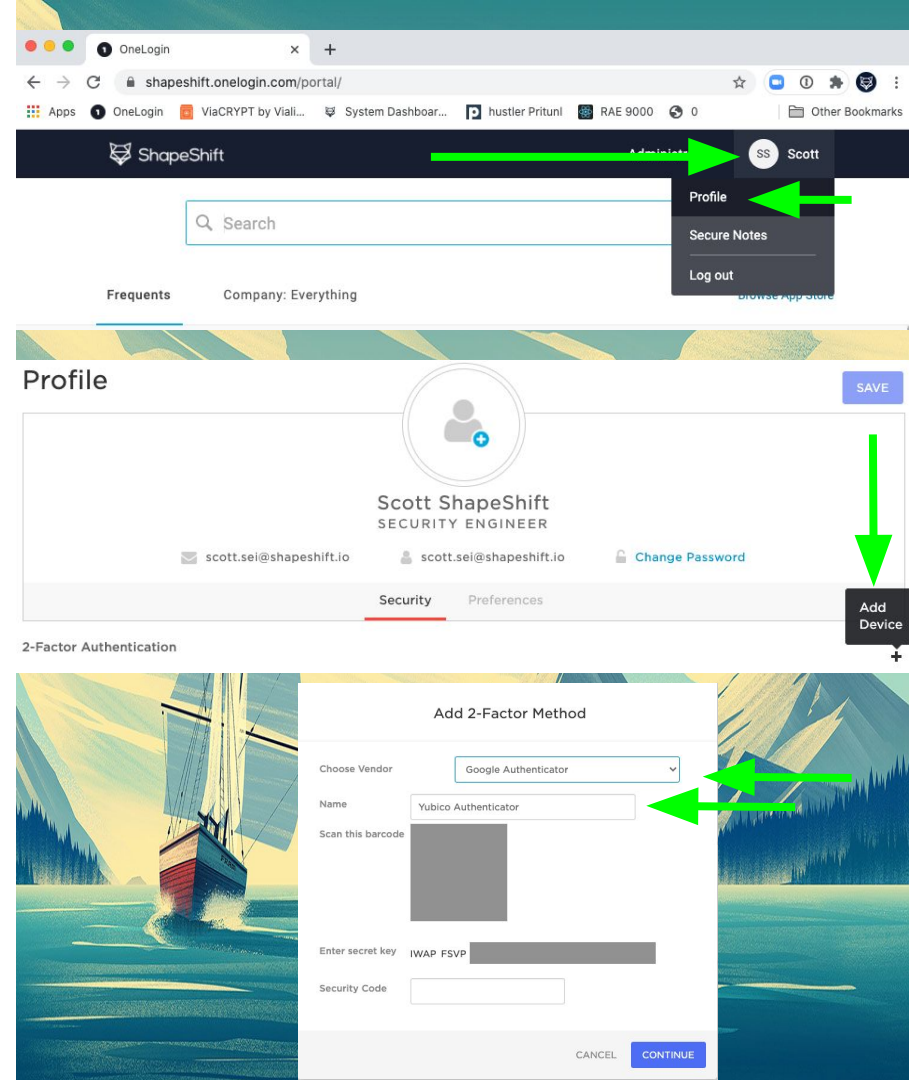
Set Up OneLogin

- Login to OneLogin
 - (<https://shapeshift.onelogin.com/>)
- Username: first.las@shapeshift.io
- Password: (will be provided via foxcry.pt)
- Insert Yubikey (Tap when prompted)






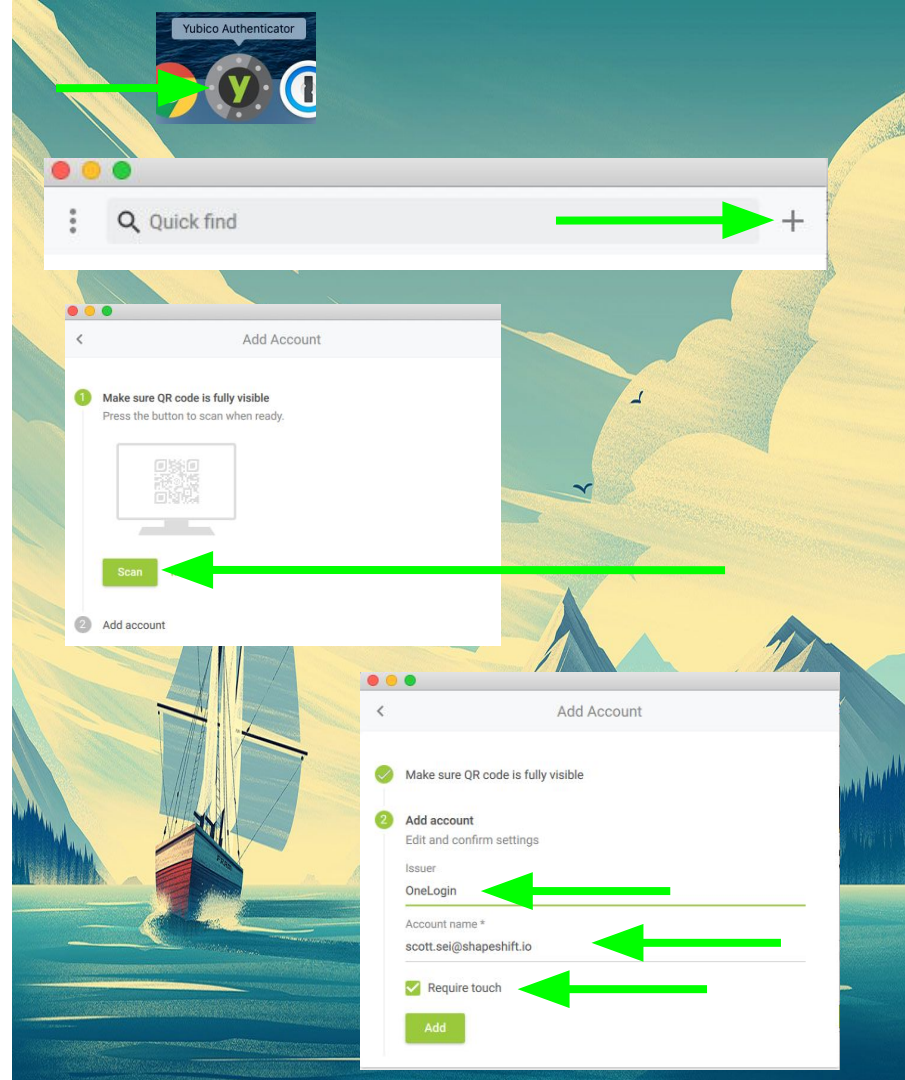
Set Up OneLogin 2FA

- Log into OneLogin
 - (<https://shapeshift.onelogin.com/>)
- At top-right corner, click Name → Profile
- Click on Add Device (+)
- Add 2-Factor Method:
 - Vendor: Google Authenticator
 - Name: Yubico Authenticator




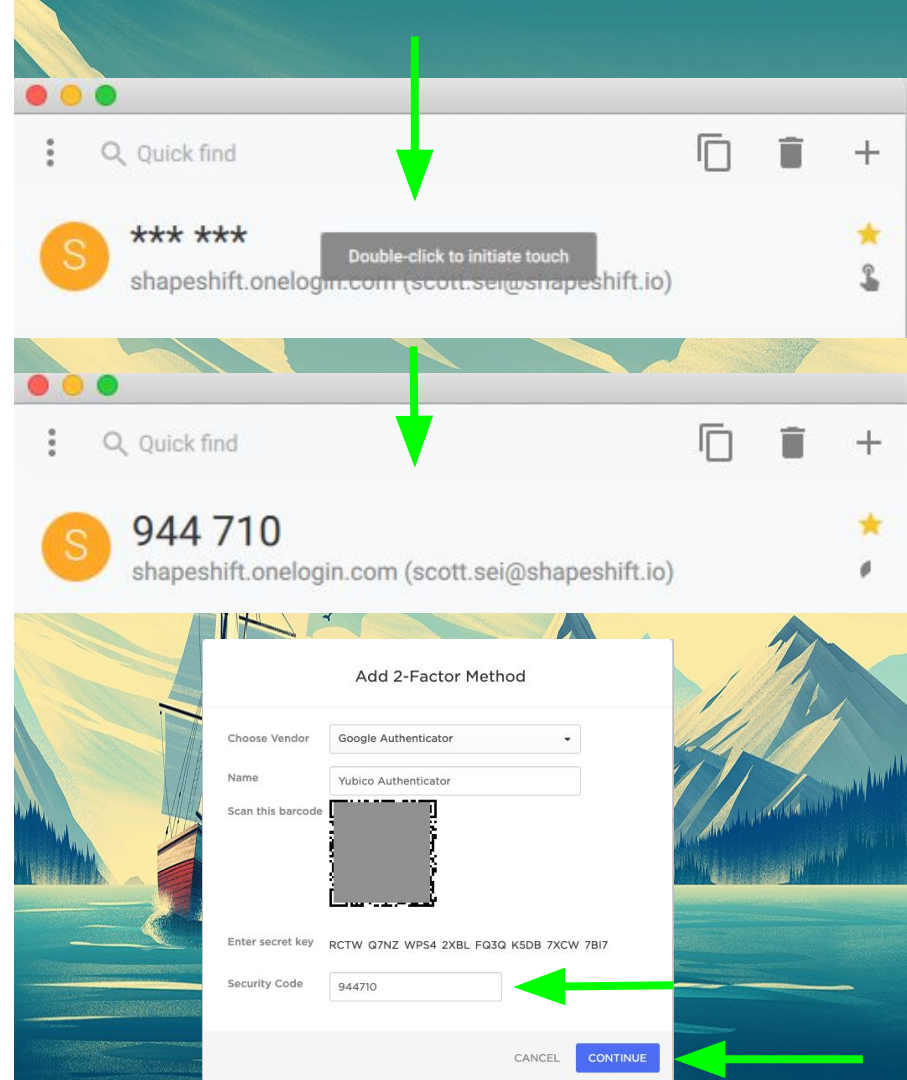
Set Up OneLogin 2FA (continued)

- Insert your Yubikey
- Launch Yubico Authenticator
- Click the  to add a authenticator
- Click 
- Confirm Details:
 - Issuer: OneLogin
 - Account Name: first.las@shapeshift.io
 - Require touch ☒
- Click 



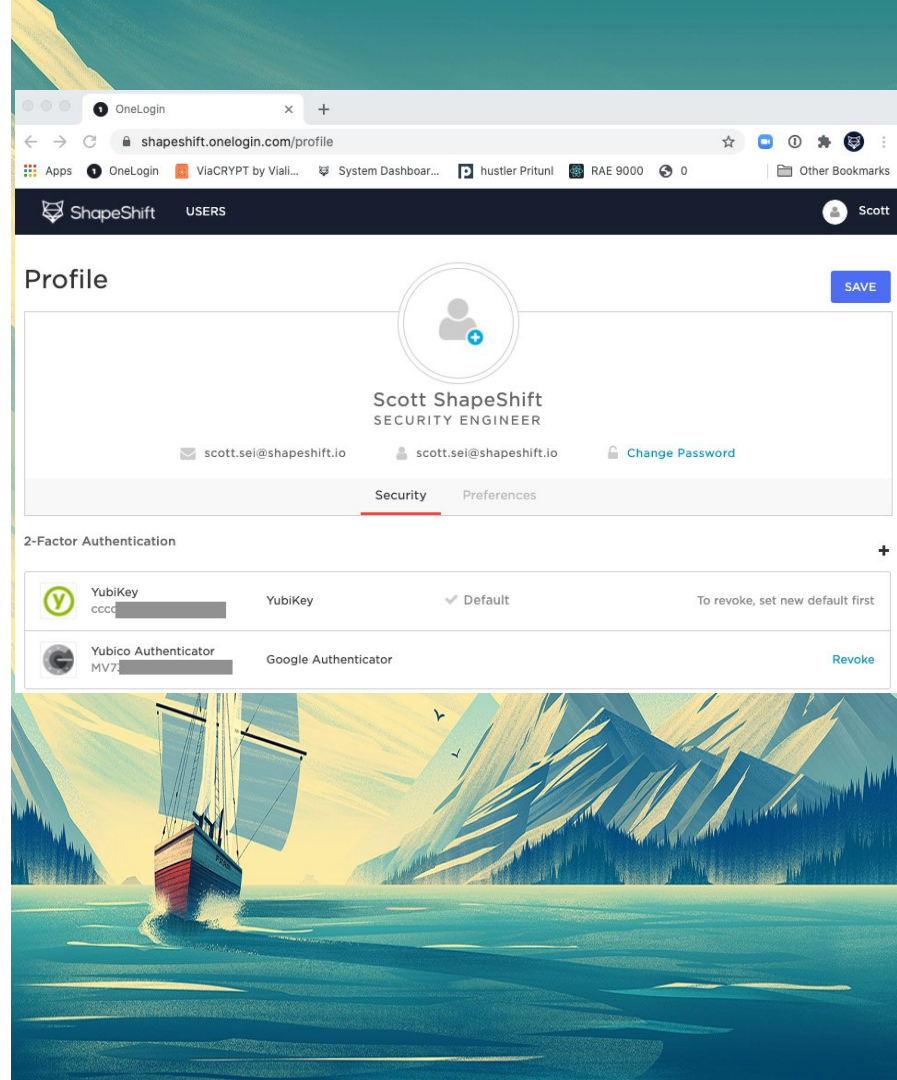
Set Up OneLogin 2FA (continued)

- Double Click the new OTP code for OneLogin
- Tap your Yubikey to reveal the code
- Copy code to the “OneLogin Add 2-Factor Method” window
- Click 



Set Up OneLogin 2FA (continued)

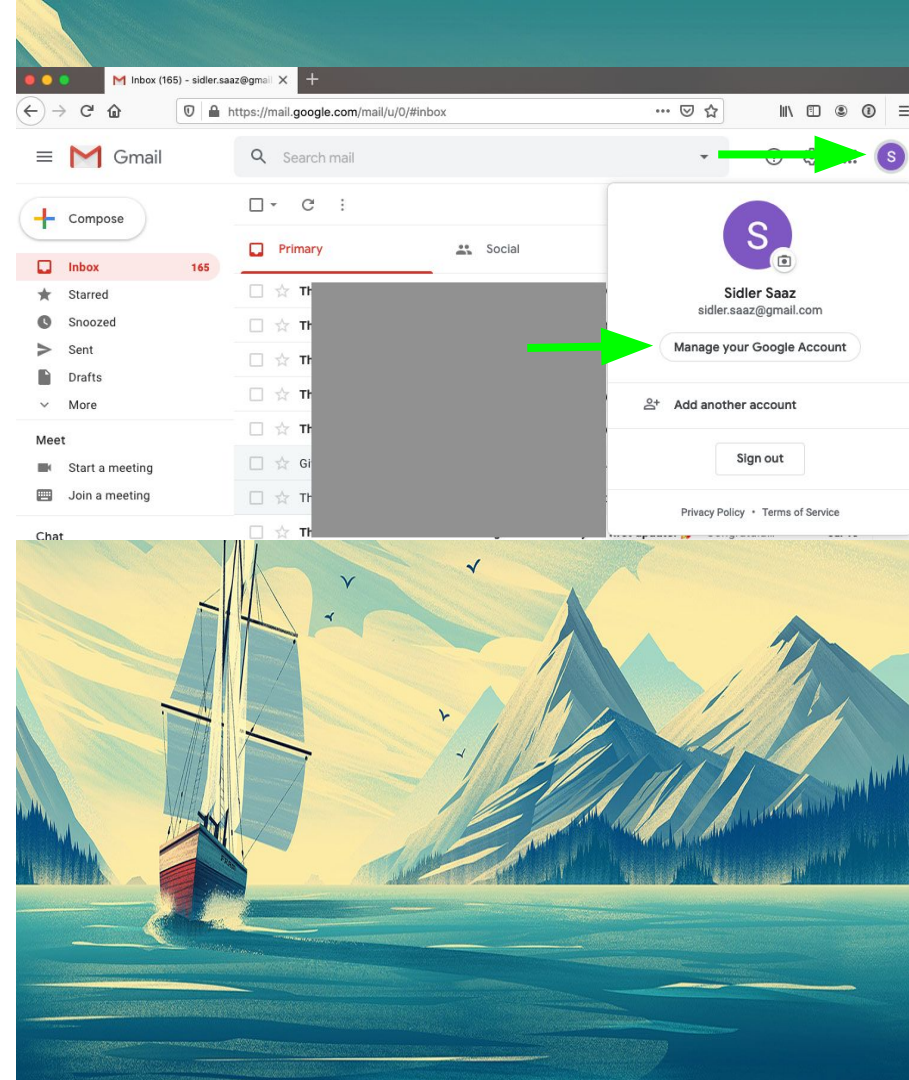
- Verify your settings look correct on the OneLogin Profile page
- You should have TWO forms of 2-Factor:
 - Yubikey
 - Yubico Authenticator



Gmail Alias

Update Email Alias Security Settings :

- Login to Google Alias account
 - At top-right, click your avatar circle
 - Click "Manage your Google Account"

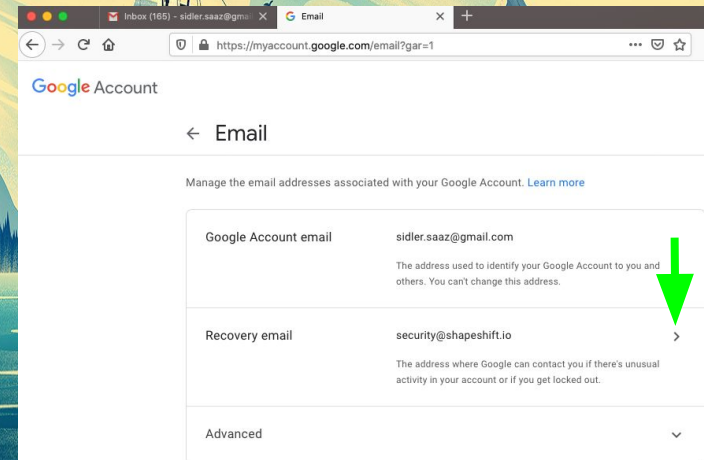
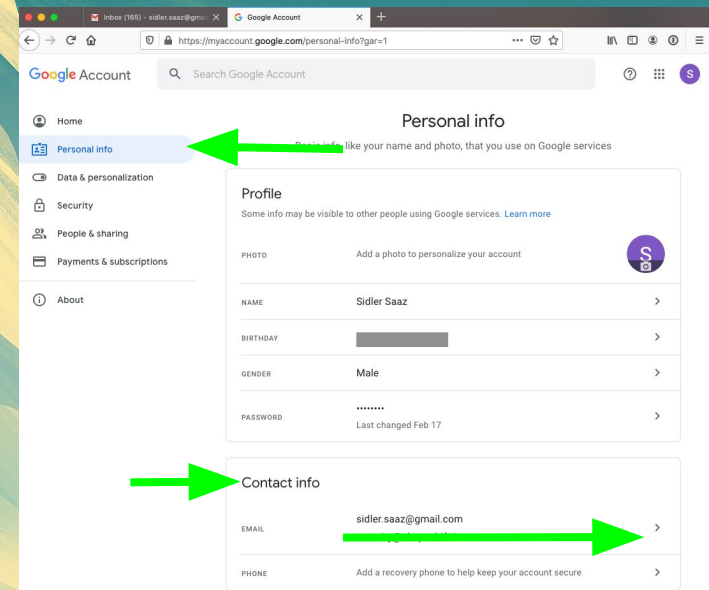


Gmail Alias (continued)

Add a recovery email to your Alias account:

- Click “Personal Info” → “Contact info”
 - Click “Email” → “Recovery email”

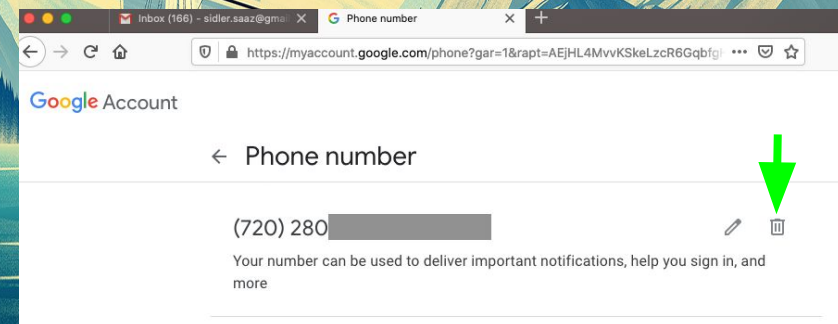
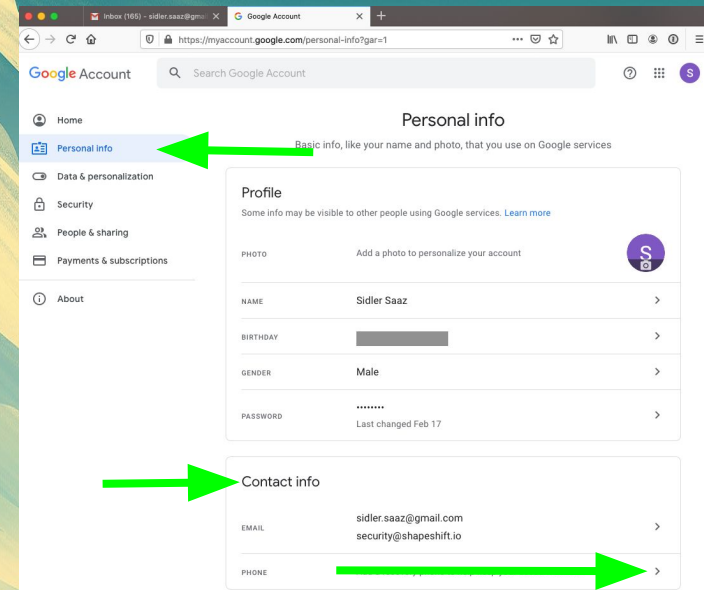
Add security@shapeshift.io



Gmail Alias (continued)

Remove all other recovery options:

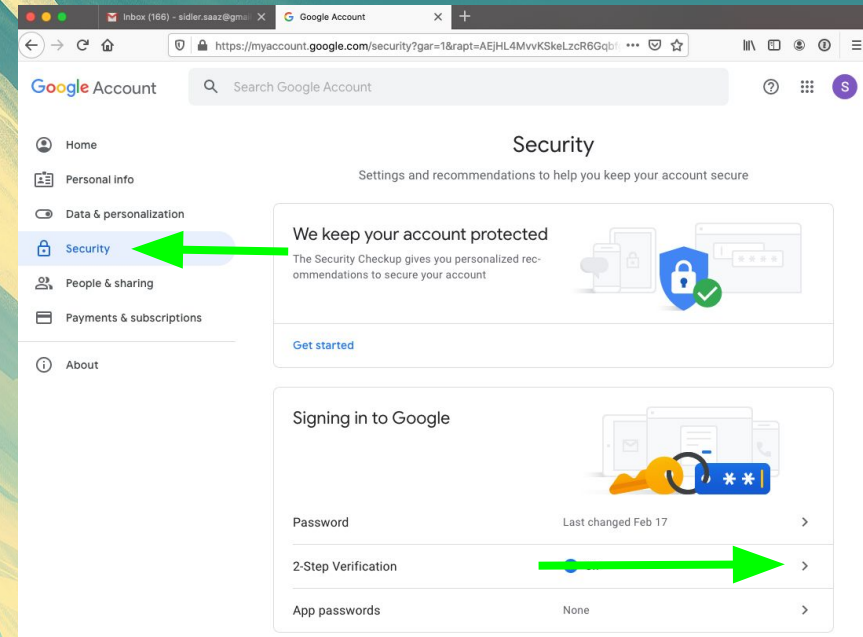
- Go back to "Contact Info" → "Phone"
- Remove phone number from account
- Remove any other recovery method



Gmail Alias (continue)

Enable 2-Step Verification

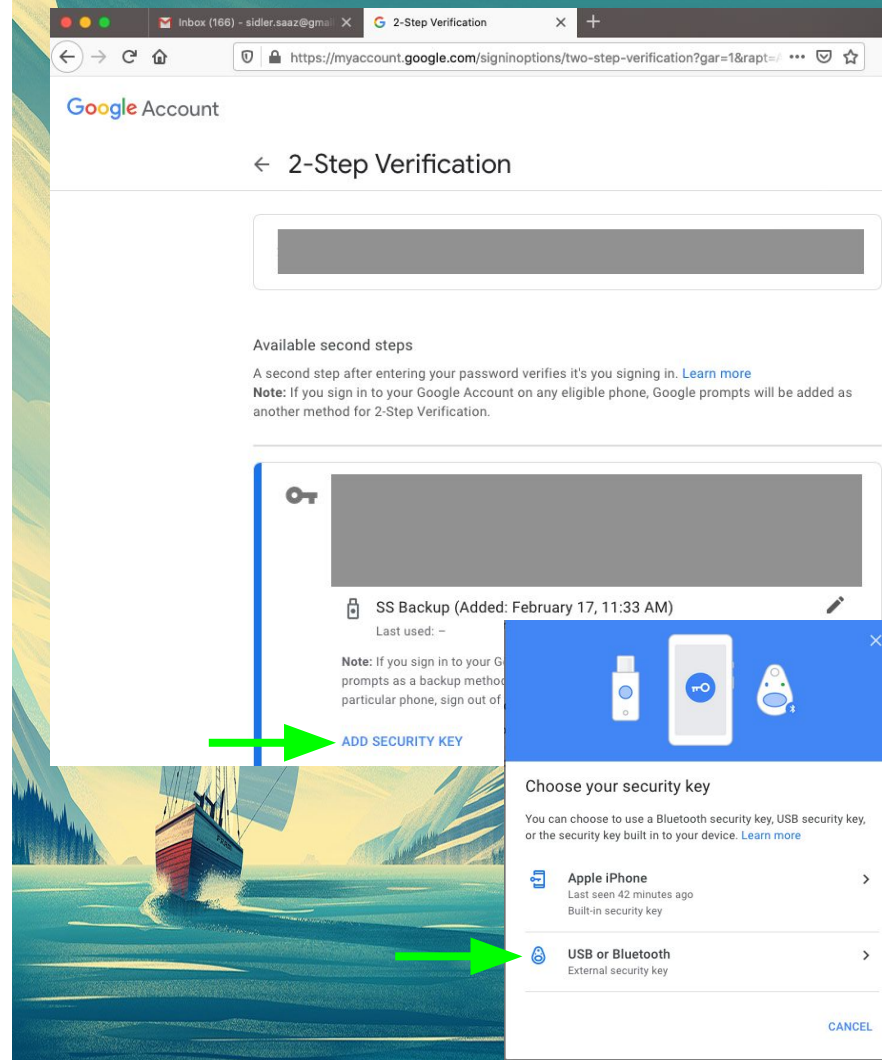
- Go Back to "Security"
- Go to "2 Step Verification"



Gmail Alias (continue)

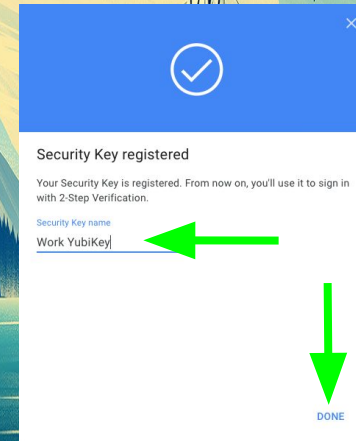
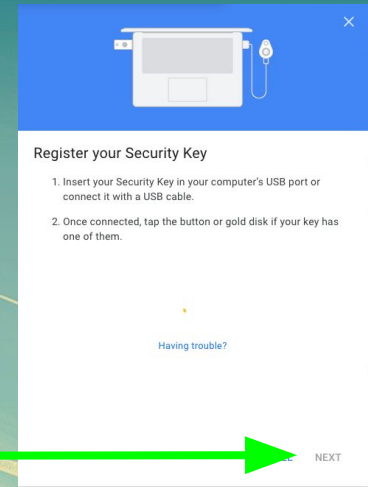
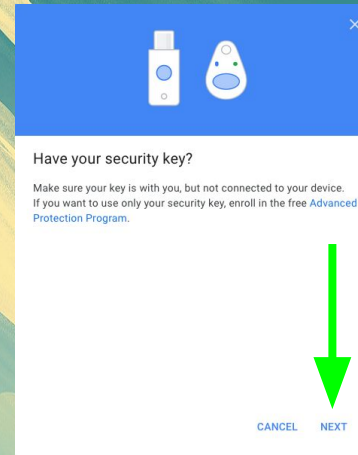
Add your Yubikey:

- Go to “Add Security key”
- Select USB or Bluetooth (External security key)



Gmail Alias (continued)

- Insert Yubikey
- Click **NEXT**
- Tap Yubikey
- Click **NEXT**
- Name your Security Key:
 - e.g. "Work Yubikey"
- Click **DONE**



Gmail Alias (continued)

- If the new hire an engineer they need a npmjs.org account?
- npm is the package manager for Node.js
- Post a message in #devops:
Please generate an npmjs token for *alias*



Set Up Pritunl

Pritunl is our corporate VPN that is required to access our internal resources and environments.

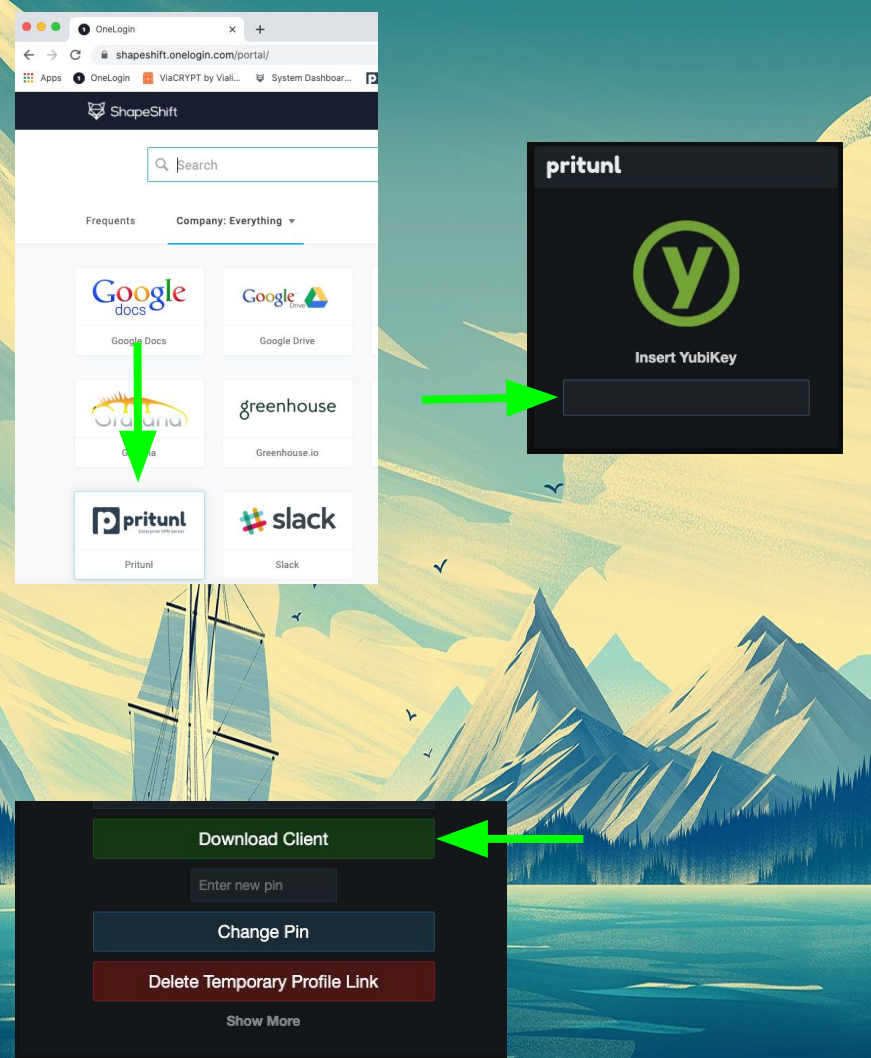
Some important sites that require the VPN:

- <redacted>
- <redacted>
- Staging / Development environments
- Any/all internal admin tools



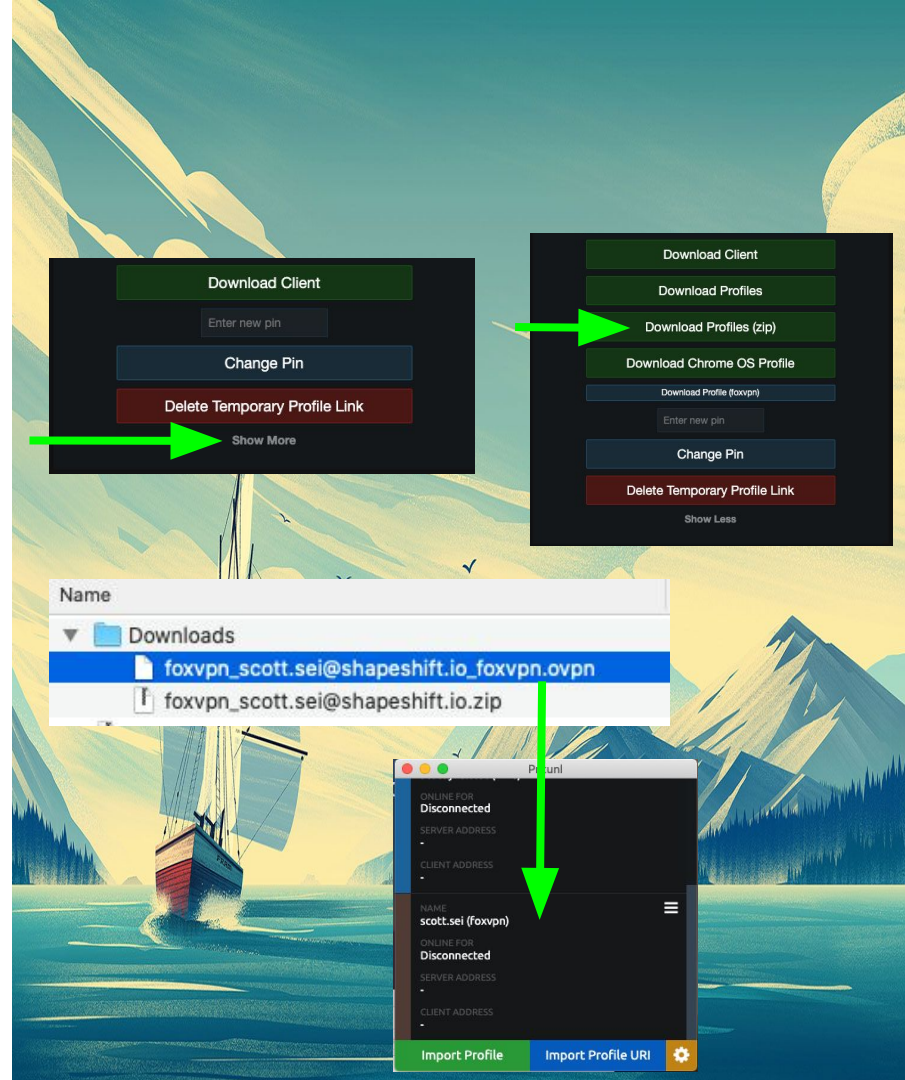
Install Pritunl Client

- Log into OneLogin
 - (<https://shapeshift.onelogin.com/>)
- Click the Pritunl badge
 - (Must be in the office)
- Insert Yubikey and Tap to authenticate
- Click Download Client
- Double click the installer to install the client
 - (use defaults)





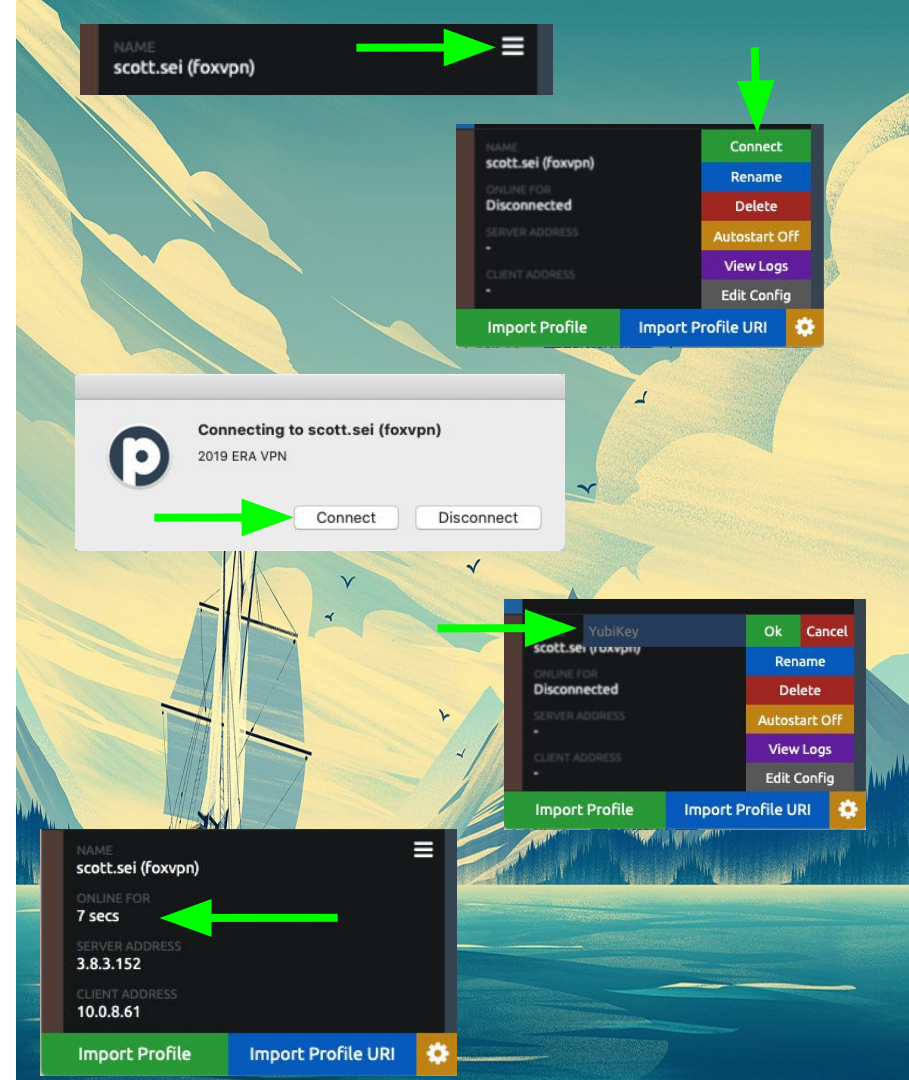
Install Pritunl Profile

- Click on Show More
- Click on Download Profiles (zip)
- Unzip the file (double click)
- Drag foxvpn_first.las@shapeshift.io_foxvpn.ovpn onto the Pritunl application



Test Pritunl

- Click on the  to connect
- Click 
- Click “Connect” on the pop up
- Tap your Yubikey into the textbox
- Verify you’re connected
 - Online For...



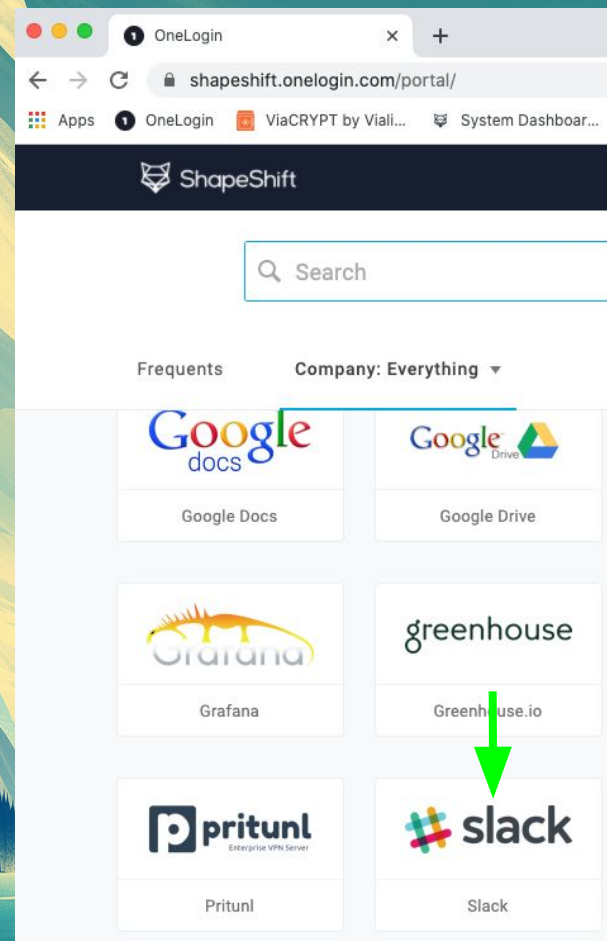
Install Slack

- Slack is a communication tool ShapeShift uses for collaboration and coordination.
- You can communicate as a group through channels or privately via “direct messaging”



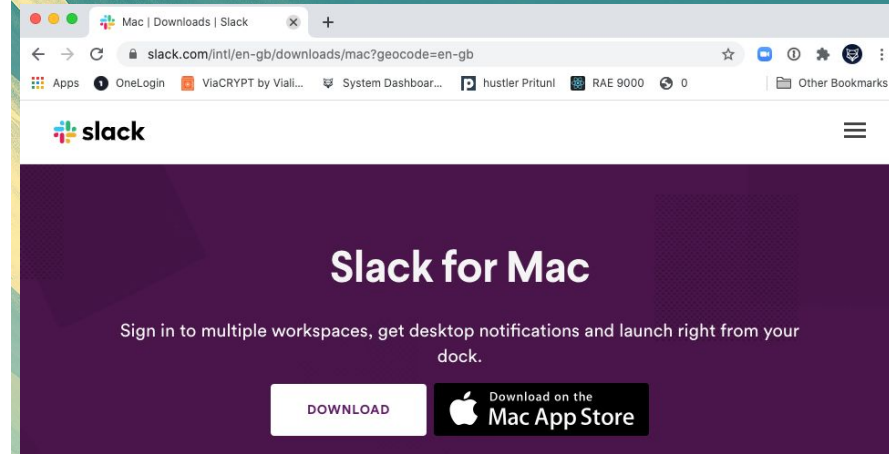
Slack Installation

- Login to OneLogin
(<https://shapeshift.onelogin.com/>)
- Click the Slack badge to login
- Workspace: foxcookieco.slack.com



Install Slack (continued)

- Go to <https://slack.com/downloads>
- Click Download
- Drag Slack to Applications
- Double Click to Open
- Recommended:
 - Keep Slack in your macOS Dock



Questions

