

1Password

1Password is a password manager used to store all of the companies shared and employee specific passwords.

- [Enrollment Process](#)
- [Free Family Subscription Redemption](#)
- [Accessing Your Account](#)
 - [Accessing 1Password](#)
 - [Signing in for the First Time](#)
- [Using 1Password](#)
 - [Vault Structure](#)
 - [Accessing a Vault](#)
 - [Adding a Password](#)
 - [Adding One-Time Passwords](#)
 - [Working with Tags](#)
 - [Conventions & Requirements](#)
 - [Google Chrome Extension \(Optional\)](#)
 - [Dark Web Monitoring](#)
- [Troubleshooting](#)
 - [Resetting Your Master Password](#)

Enrollment Process

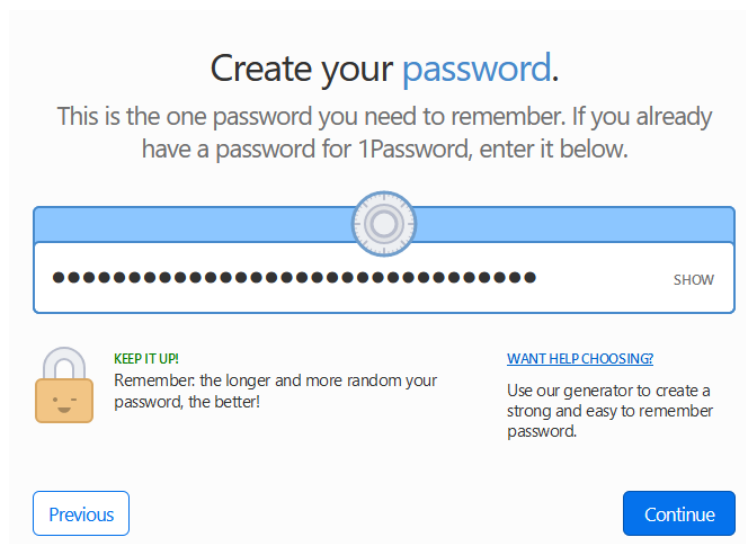
This article will walk you through enrolling in 1Password.

If you did not receive a 1Password enrollment email, please contact [IT Support](#).

Enrollment

Within the email, please click the **Join Now** button to start the enrollment process. A new browser window will appear, requesting that you create an account password. This password is known as the *Master Password* by 1Password. The password should have a length of at least 24 characters. As with your domain password it's recommend you use a long sentence or a series of memorable words. Additionally, **do not use your domain password**. This ensures your 1Password account remains secure if your domain account is ever compromised.

Visit <https://www.useapassphrase.com/> for password ideas.

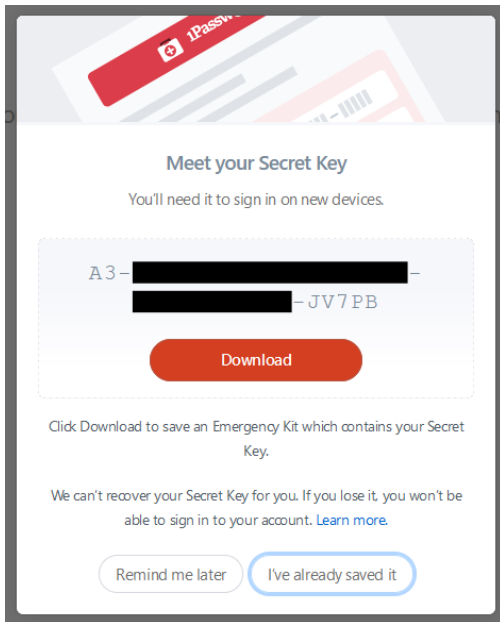


The screenshot shows the 1Password enrollment interface. At the top, it says "Create your password." followed by a subtext: "This is the one password you need to remember. If you already have a password for 1Password, enter it below." Below this is a password input field with a blue header bar and a circular icon on the right. The field contains 24 black dots. To the right of the dots is a "SHOW" link. Below the input field, there are two columns of text. The left column has a padlock icon and the text "KEEP IT UP! Remember: the longer and more random your password, the better!". The right column has a link "WANT HELP CHOOSING?" and the text "Use our generator to create a strong and easy to remember password." At the bottom, there are two buttons: "Previous" on the left and "Continue" on the right.

Please input your password then select **Continue**.

1Password Emergency Kit

With your password chosen, 1Password will now provide you with a link to download your *1Password Emergency Kit*. This document is important as it requires all of the information you need when signing onto a new device for the first time.



For security reasons, please **DO NOT** store this document in electronic form, whether on the file server or your laptop. Instead please download the 1Password Emergency Kit, print the document out and immediately delete the electronic version.

If located outside of the lower mainland please store the printed copy in a secure location. For employees located within the lower mainland, please provide this document to Administration so it can be securely stored within the office safe.

The Emergency Kit provides a spot to write your Master Password. Please **DO NOT** write down your master password. If this password is lost, your account can be easily recovered by IT.

When complete select **I've already saved it**.

Final Steps

Enrollment has been completed! Once the IT department has approved your account, you'll receive a welcome email from 1Password.

Welcome to 1Password

Here are your account details. You'll need them to sign in to 1Password.



Your sign-in address:

<https://georgebellconsulting.1password.com>

Your email address:

tyler.rasmussen@georgeandbell.com

Your Secret Key:

It's in your [Emergency Kit](#)

You're now ready to sign into 1Password using the 1Password app. Please see [Signing in for the First Time](#) for instructions.

Free Family Subscription Redemption

As part of your 1Password subscription, each employee can redeem a free [1Password Families](#) membership. Using this complimentary subscription, you and your family can use the 1Password password manager free-of-charge for up to five family members.

For more information, please see 1Password's [Support Article](#) regarding the offering.

Redemption

To redeem your free 1Password Families membership, please:

1. Sign into your 1Password account via a [web browser](#).
2. Click on your name within the top right-hand corner and select **My Profile**.
3. Scroll to the bottom of the page and select **Redeem Now**.

Free 1Password Families Membership

Use 1Password at home too. Redeem your free 1Password Families membership, courtesy of your business.



4. Select either **Sign Up** to create a new 1Password account or choose **Apply to existing account** if you already have a 1Password subscription.

Please only contact IT Support if you're experiencing issues redeeming your free membership. For any issues related to configuring 1Password on personal devices, please reach out to [1Password Support](#) directly.

Privacy

As documented by 1Password themselves, please know George & Bell cannot access nor has any control over any credentials stored within your 1Password Families membership.

Linked family accounts share only their subscription status with a business account. Ownership and access rights aren't shared. A linked family account belongs to the family organizer, and the business can't access or manage it.

Leaving the Company

This offering is only valid during your employment with George & Bell Consulting. Upon leaving the company, 1Password ask that you start paying their standard [1Password Families membership rate](#) if you wish to continue using the service.

Accessing Your Account

Accessing 1Password

1Password has a variety of ways it can be access and used. These include:

- Google Chrome Extension
- Web Browser
- Desktop App
- Mobile App

If just starting with 1Password, its recommended you start with the Desktop App as its the easiest and most intuitive method of accessing your credentials. Below are instructions on signing in via the Desktop App.

Desktop App

The Desktop app is installed on all work laptops. If not found, please contact [IT Support](#).

Automatically deployed and installed on all laptops, you can access your account through the 1Password Desktop App.

1. Within the Start Menu open the 1Password app.
2. See the [Signing in for the First Time](#) article for information on signing in.

Google Chrome Extension

Available on [Google's Chrome Web Store](#), this extension allows you to access 1Password via a click of a button in Google Chrome.

1. In Google Chrome, click [here](#) to view the 1Password Chrome Extension.
2. Select **Add to Chrome** to install the extension.
3. See the [Signing in for the First Time](#) article for information on signing in.

For more information on using the Google Chrome extension, please see [this article](#).

Web Browser

Through any web browser, you can logon to your account at <https://georgeandbellconsulting.1password.com>.

1. Within the web browser of your choice, browse to <https://georgeandbellconsulting.1password.com..>
2. See the [Signing in for the First Time](#) article for information on signing in.

Mobile App


Available via the Google Play Store (Android) or App Store (iPhone), the 1Password app allow you to access and view your credentials via your mobile phone.

1. Open the **Google Play Store** or **App Store** depending on whether you use an Android or iPhone.
2. Search for "1Password 8" and install the app available from *AgileBits Inc.*
3. See the [Signing in for the First Time](#) article for information on signing in.

Signing in for the First Time


Preparations

Prior to starting the sign-in process, please ensure you have the *1Password Emergency Kit* handy. If located near the Vancouver office, please ask IT or Administration who can collect and provide you with the document from the office safe.

 **1Password** Emergency Kit

Created for Wendy Appleseed on 2022-10-07.

1Password Account Details

SIGN-IN ADDRESS	<input type="text" value="https://teamagilebits.1password.com"/>
EMAIL ADDRESS	<input type="text" value="wendy_appleseed@agilebits.com"/>
SECRET KEY	<input type="text" value="A3-FSHJNM-7T85AC-VC83W-7NTCN-457SS-BA3H1"/> 
PASSWORD	<input type="password"/>

Need help?
Contact 1Password at:
support@1password.com



Setup Code
Scan this code from the 1Password apps to set up your account quickly and easily.

To successfully sign into your account, you'll need the following information:

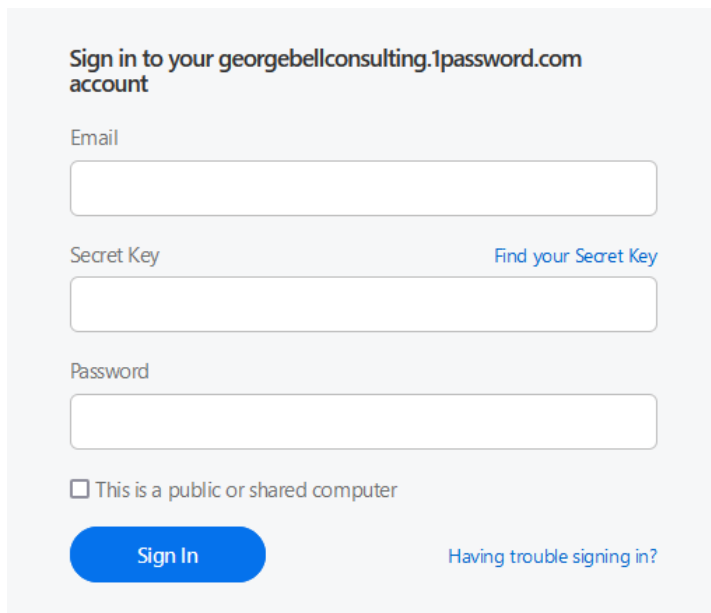
- Sign-in Address *
- Email address
- 1Password Secret Key *
- 1Password Master Password
- Successfully complete a Duo Authentication Prompt.

* Found on the *1Password Emergency Kit*

Signing In

1Password has a variety of options to access your saved passwords including through a web browser, desktop app, mobile app and Google Chrome extension. The sign-in process is the same no matter your preferred method of access.

On first sign-in, you'll be asked for some additional information outside of your username and password. Below is a walk-through of completing this process. Once completed, subsequent sign-ins will only require your 1Password Master Password.



The screenshot shows a sign-in form for the account **georgebellconsulting.1password.com**. It includes three input fields: **Email**, **Secret Key**, and **Password**. A link [Find your Secret Key](#) is located next to the Secret Key field. Below the fields is a checkbox labeled **This is a public or shared computer**. At the bottom left is a blue **Sign In** button, and at the bottom right is a link [Having trouble signing in?](#).

On the logon screen please enter your Email, Secret Key and 1Password Master Password. The Secret Key can be found within the 1Password Emergency Kit collected at the start of this guide. The requested password is your 1Password Master Password created when enrolling in the 1Password service.

Remember unlike most George & Bell services, your Master Password is unique and not used elsewhere in the organization.

When complete press **Sign In** to initiate a **Duo Authentication Request**.



Check for a Duo Push

Verify it's you by approving the notification...

Sent to "iOS" (••••••••4910)



[Other options](#)

[Need help?](#)

Secured by Duo

Once verified, you will be successfully signed in. On subsequent sign-in's you will only be asked for your 1Password Master Password.

Using 1Password

Vault Structure

Passwords are stored in containers known as Vaults. Vaults can be thought of as a folder with its own set of permissions controlling access to the *files* (aka. passwords) stored within. Anyone with access to the vault can see/modify/delete passwords created by themselves and others. In 1Password, three types of vaults exist:

- Private
- Personal (exist, please do not use)
- Shared

Private Vault

The Private vault is a built-in vault that allows you to store credentials only you should see. Accessible only to you, this vault is automatically created when you enrolled in 1Password; it cannot be deleted.

IT Support can access Private vaults if authorized by the partners or the employee who owns the Private vault.

Shared Vaults

Shared vaults are vaults created and managed by IT Support that hold credentials for specific departments or groups of employees. These vaults cannot be deleted or modified, rather employees can only add/remove/change passwords stored within based upon their access.

Currently the following shared vaults exist:

- GB Administration
- GB Corporate
- GB Benefits
- GB Investments
- GB Pension
- GB Pen Invest
- GB Shared
- SISS Corporate
- SISS Shared

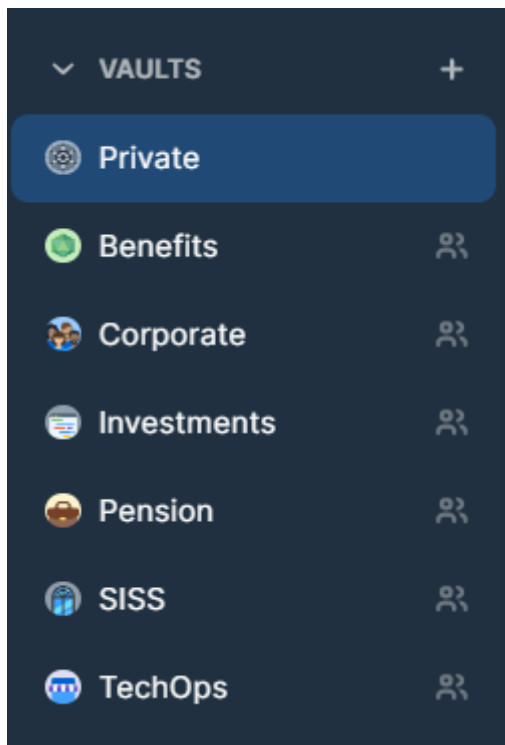
As with Private and Personal vaults, Shared vaults will appear within the left-hand column of the 1Password app under the Vaults heading.

Accessing a Vault

Using the 1Password app, vaults can be access via the left-hand sidebar. As discussed in the Vault Structure article, each vault contains the shared credentials for each department, with an exception being the Private Vault which only you have access too.

If you are missing a vault, please speak with your manager.

1. Open the **1Password app** and login.
2. Within the left-hand sidebar select the vault you'd like to view.

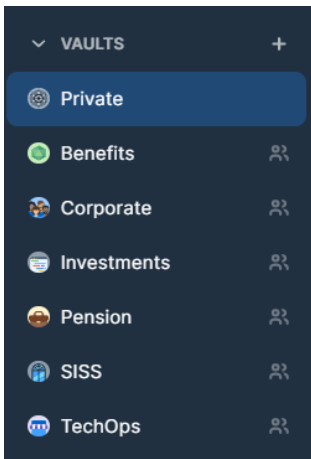


Adding a Password

This article will walk you through adding a new password into the 1Password app. We'll start by determining what type of login we would like to save then move onto adding the login details.

If using the 1Password extension or mobile app the basic steps are the same however the UI may look different.

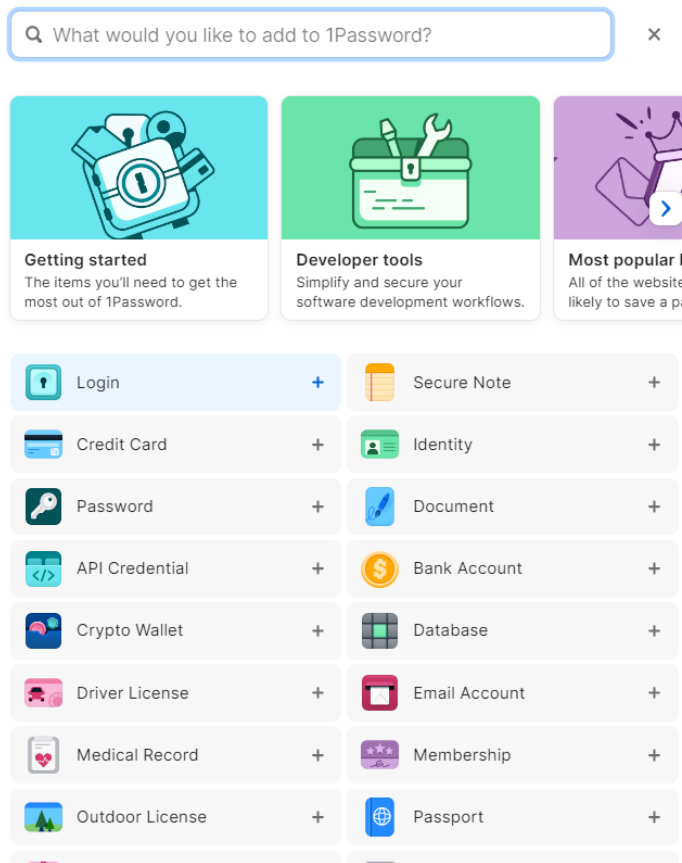
1. Logon to the **1Password app**.
2. Within the left-hand sidebar, select the vault you'd like the password to be saved in.



3. In the top right-hand corner, select **+ New Item**.

+ New Item

4. Select the type of credential you'd like to add. If unsure select **Login** (the most common type).




Fill in the Details

A window will appear asking for the account details. We'll go through each section separately.

While overwhelming, only a few fields need to be filled in.

← New Item ×

 My Service

username

myusername

password

.....

website

https://examplewebsite.com

+ add another website



+ add more

notes

Add any notes about this item here.


tags

+ Add tag

 George & Bell Consulting |  Private

Save

1. Enter what you'd like to call this account, for example the company name.

 My Service

2. Enter the account's username and password.

username

myusername

password

.....

3. Enter the account holder's website (optional but helpful).

website

https://examplewebsite.com

+ add another website

4. Add billing code tags onto this new login.

Tags help organize the passwords stored within a Vault. For more information see [Working with Tags](#).

tags

Vendors ▾

+ Add tag

5. Lastly, click **Save** to save the new login.

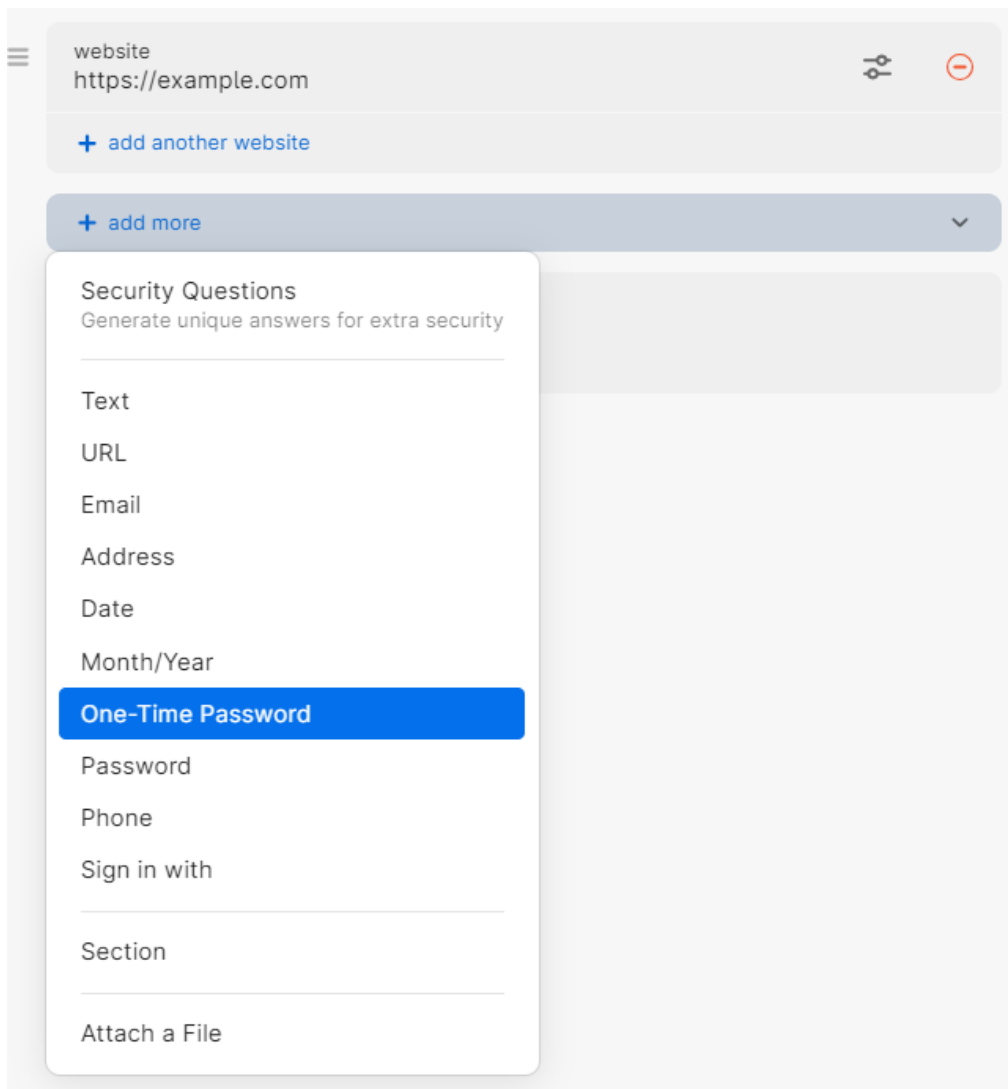
Adding One-Time Passwords

One-Time Passwords (OTP) are a common type of multi-factor authentication that uses a combination of a passphrase (just a random set of characters) and the time to generate a ever changing 6-digit passcode. The service you're logging into is then able to use the time and the six digit code to determine the original passphrase, validating your identity.

To add a One-Time Password start by selecting the credential you'd like to add the One-Time Password onto. Choose **Edit** in the top right-hand corner. A new window will appear, allowing you to edit the credential.



Select **Add more** and choose **One-Time Password**. A new field will appear asking for the passcode.

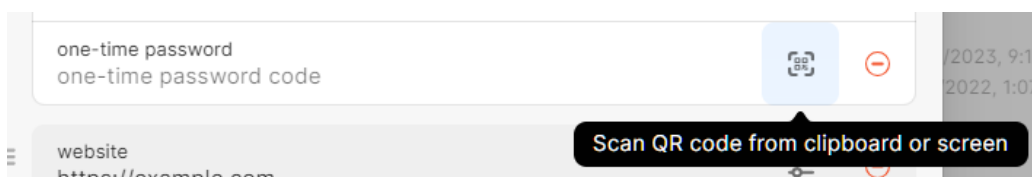


Password provides two different methods of entering in the passcode, via QR code or by manually entering in the One-Time Password passphrase. By default most sites will provide you with a QR code, however sometime reading the QR code fails and entering the passphrase in manually may be the best option.

QR Code

To scan and have the passphrase entered into the 1Password One-Time Password field, please:

1. Ensure that the QR Code is visible on the screen when 1Password is open.
2. Press the Scan symbol to have 1Password read and fill in the passphrase.



Manually Enter the Passphrase

Alternatively, some sites (unfortunately not all) will allow you to see the underlying passphrase instead of the QR Code. If this is the case, simply copy and paste the passphrase into the One-Time Password field in 1Password.

one-time password

NyYv7hYiMd6RDnstE6ynEumX



4. Select **Save**. You should now see a rotating One-Time Password for your credential.



Example Logon

username


username

password

.....

Terrible

one-time password

998 • 468  01

website

<https://example.com>

Working with Tags

In 1Password, tags are labels that you can assign to passwords in your vault. They can be used to organize your items in a more flexible and customizable way than traditional hierarchical methods (folders for example).

Tags can be applied to any type of item in your vault, such as passwords, credit cards and secure notes. You can create your own tags or use existing ones, and assign multiple tags to an item if desired.

Please see 1Password's [Support Article](#) for more information on using tags.

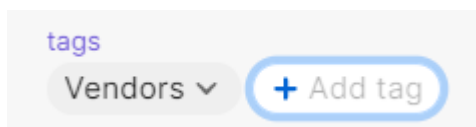
Applying a Tag

The following is a quick how-to on adding a tag to an existing item.

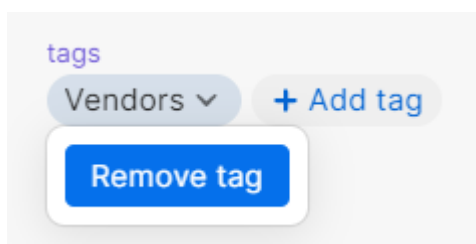
1. Open the **1Password app**.
2. Select the **item** you'd like to add the tag too.
3. Select **Edit** within the top-right hand corner.



4. Under the *Tag* section, select **Add Tag** and type in the tag you wish to add.



5. If you wish to remove a tag, select the tag a choose **Remove Tag**.



Conventions & Requirements

Separate Logins for Each Site

Each site/username/password combo should be a separate login. This allows autofill to work correctly display and autofill the login details when searched/presented. Ex. BlackRock.

Security Questions

When adding security questions information to a login, ensure this information is added to the *Security Question* field and not a generic *text* or *notes* field. This will allow autofill to correctly locate and autofill the information when its requested.

To add a *Security Question* field to a login, select add more and choose **Security Question** from the drop-down.

The screenshot shows the 1Password 'Login' interface. At the top, there's a 'Login' header with a key icon. Below it are two input fields: 'username' and 'password'. Underneath these is a 'website' field containing 'https://example.com'. To the right of the website field are icons for a link and a warning. Below the website field is a '+ add another website' link. Further down is a '+ add more' button with a dropdown arrow. This dropdown menu is open, showing a list of options: 'Security Questions' (highlighted in blue), 'Text', 'URL', 'Email', 'Address', 'Date', 'Month/Year', 'One-Time Password', 'Password', 'Phone', 'Sign in with', 'Section', and 'Attach a File'. The 'Security Questions' option has a subtext: 'Generate unique answers for extra security'.

Tagging

When adding tags to a logon entry, **always** use the client billing codes for the tags.

- Sub-codes/suffixes are currently excluded (hyphenated billing codes only in use where the hyphenation is for a SEPARATE client).

Login Items with Multiple Data Room/Managers

When creating login items that have multiple data rooms and/or managers:

- Tag with CLIENT manager names (manager tags not needed otherwise). i.e., manager tags should only be used for items with multiple managers for ease of searchability.
 - Sometimes data room access is granted when we're doing a search. These managers/funds should not be tagged; just include a tag for the client for which the search is being conducted.
 - myMAWER is Mawer's proprietary/dedicated site and contains Mawer in the title, so a "Mawer" tag need not be included.
- Create new Section = Data Room, Text "title" = Fund/Manager name, Text = client billing codes.

Multi-Factor Authentication

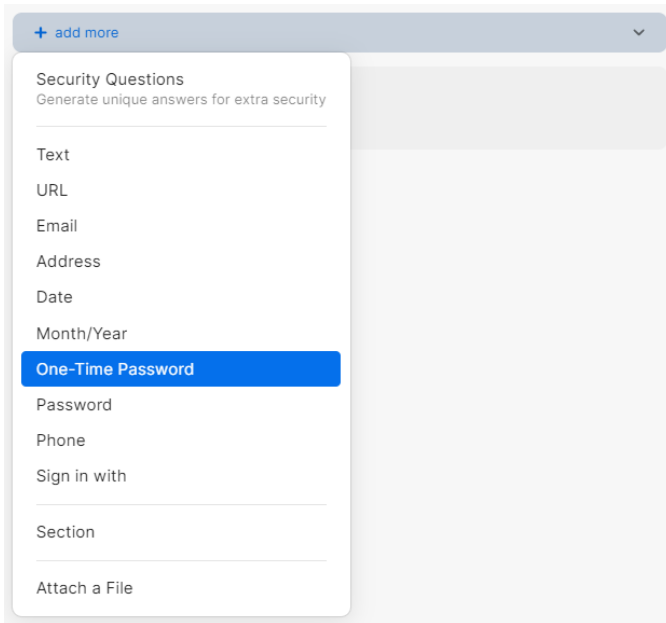
It's preferred that whenever possible the built-in 1Password MFA authentication mechanism be used for storing and reading MFA codes. If not available, configure MFA to email investmentreports@georgeandbell.com.

As a last resort, use your personal Duo, Microsoft Authentication apps or SMS. These options are not preferable as it does not allow anyone else to logon to the account without your device.

To add a MFA code onto a 1Password logon item, please:

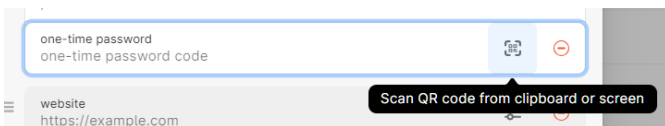
1. Choose the logon item you'd like to add the MFA code to.
2. Select **Edit** within the top right-hand corner to edit the item.

3. Select **add more** and choose **One-Time Password**.



4. Select the little square symbol to have the QR code scanned from the screen.

If not working, many sites allow you to copy/paste the code directly into the field.



Password Creation

By default 1Password uses their *Smart Password* generator, which generates a password as a random series of characters. This is the preferred option, however at times may not meet the password requirements of the site or it may be preferable to have a password that's memorable. To change how 1Password generates the password:

1. Under the logon item you're editing/creating select the password field.
2. 1Password should automatically prompt to **Create a New Password**. Select this option.
3. In the resulting drop-down update **Type** to you're preferred password generating mechanism.

username

username

password

password

Cancel

↺

Use

tzhvRxqGZ4sED8dhGuMwz7PC

Type

Random Password ↕

Characters

Random Password ✓

Numbers

Memorable Password

Symbols

PIN Code

toggle

tags

...




Google Chrome Extension (Optional)

Installing Extension


The Google Chrome 1Password extension is available and can be installed via the Google Chrome web store. To install the extension, please:

1. Browse to the [1Password Extension](#) page on the Google Chrome Web Store.
2. Select **Add to Chrome**, to install the extension.

By default, the extension may be hidden from view. To have the extension always conveniently available, perform the following steps:

1. Press the Extension icon  within the top-right hand corner.
2. Select the Pin icon  directly next to the *1Password - Password Manager* extension.
3. The extension should now be immediately available in the top right-hand corner . 

Sign In

Before using the 1Password extension, you need to sign-in to your 1Password account. Please click on the 1Password extension  to view the 1Password sign-in page. Press **Sign In** to start the process.

For more information on how to sign-in to 1Password, please see [Accessing Your Account](#).

Dark Web Monitoring

Dark web monitoring is a service that searches for and monitors information found on the dark web. The service looks for stolen and/or leaked information, such as compromised passwords, credentials, intellectual property, and other sensitive data being shared and sold among criminals operating on the dark web. This information can include:

- Credit card details.
- Account credentials.
- PII information (name, address, phone number etc.)

If this information is found, a breach report is generated and the associated employee(s) are notified. Additionally IT is notified so immediate action can be taken if required.

FAQ

Answers to commonly asked questions.

What do I do if I receive a breach report?

Check and see if any of your accounts are at immediate risk of being accessed by an unknown person. If yes, change your password immediately and notify IT. For certain types of reports such as web scrapping unfortunately little can be done other than being vigilant as you'll be at increased risk for identify theft.

IT receives all breach reports and will reach out if concerned. If the breach is considered significant, the affected accounts may be temporary disabled with no notice to you to ensure the security of the company.

How does 1Password determine that a breach has happened?

After a company or individual has been compromised, it's common for the hacker to either:

1. Attempt to sell the information online (usually on the dark web).
2. Publicize the information.

1Password looks for these types of posts and analyzes any information collected. If information related to George & Bell Consulting is found, a breach report is generated.

I recently learned that my personal information was collected. What can I do about it?

Be vigilant as you'll be at increased risk of identity theft with your personal information publicized. Here are a few steps you can take to protect yourself:

- Monitor your credit cards and call the credit card company immediately if anything is amiss.
- Place a credit freeze on your name. This will stop any identity thieves from opening any account that includes a credit check (loans, credit card etc.).
- Don't be truthful when setting up security questions. For example, when asked what city you were born in, lie. (but do document it so you can remember it!)
- Call various providers to see if they can add additional security checks as part of verifying who you are.

If you do become the victim of identity theft, the recommended approach is to:

- notify your financial institution and the local police.
- contact the CRA at 1-800-959-8281.
- report the theft to a credit reporting agency such as Equifax or TransUnion.
- keep records of recent purchases, payments, and financial transactions.
- Call 1-800-O-Canada (1-800-622-6232) for information on how to replace identity cards such as your health card, driver's license, or SIN if necessary.

[More Information](#)

Where can I learn more about this service?

Please visit [1Password's Support](#) site.

What can I do personally if my information is released?

Monitor your credit cards and call the credit card company immediately if anything is amiss. Common signs of identity theft include:

- Receiving an application for credit in your name
Your bank informing you that they have approved/denied your application for a service you never applied too
- No longer receiving a statement and finding unusual purchases.

If extremely concerned, you can place a credit freeze on your name. This will stop any identity thieves from opening any account that includes a credit check (loans, credit card etc.).

- Don't be truthful when setting up security questions. For example, when asked what city you were born in, lie. (but do document it so you can remember it!)

- Call various providers to see if they can add additional security checks as part of verifying who you are.

Troubleshooting

Resetting Your Master Password

If you've lost access to your account due to forgetting or misplacing your 1Password Master Password, please reach out to IT Support. Once notified, IT Support will start the recovery process, allowing you to re-gain access to your account.

Resetting your password will generate a new Secret Key.