

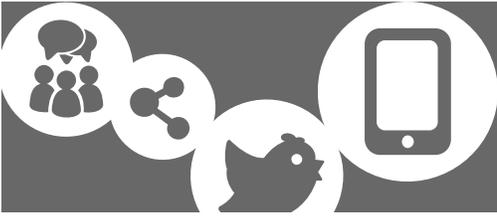


# Secure Your BigCommerce Store



## Contents

Introduction	<b>3</b>
Your Account	<b>4</b>
Users	<b>5</b>
Apps	<b>6</b>
Backups	<b>7</b>
Checklist	<b>8</b>

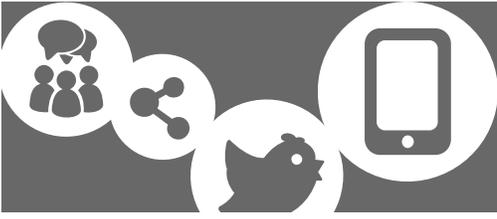


## Introduction

Your online store is extremely important. Regardless of whether your store gets 1 order per month or millions of orders per month, you need to ensure it remains safe and secure. Online e-commerce platforms like BigCommerce are great - they provide a platform for users to collaborate, work together, and for apps to add functions that aren't available natively.

Unfortunately, these additional users and apps can cause problems for store owners by accidentally deleting data, making unwanted changes, or in some cases deleting your entire store.

In the next few pages we'll cover what you can do to help improve the security of your BigCommerce store.

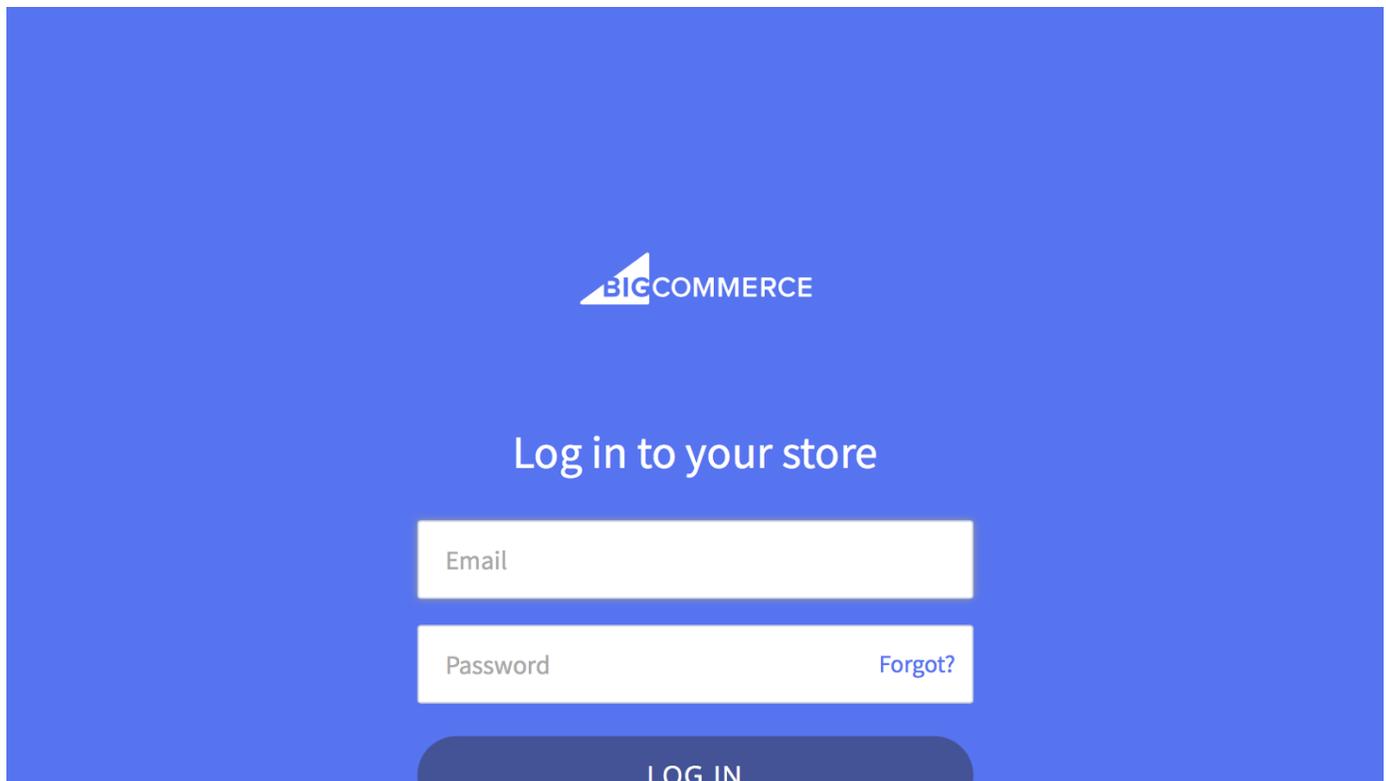


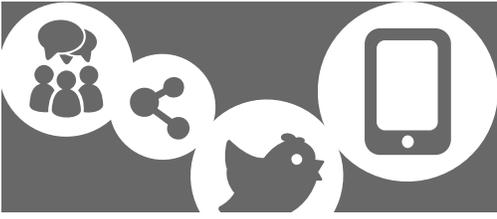
## Your Account

Your main account is the easiest way for someone to get access to your BigCommerce store and cause havoc. To prevent this, we recommend you use a very strong password that contains at least 12 characters including uppercase letters, lowercase letters, numbers and symbols. This password should be impossible to remember, so to make it easier you should use a password manager like 1Password.

1Password is designed from the ground up to be completely secure. You can read more about their security at <https://1password.com/security/>, but suffice it to say that it's a very secure system.

1Password starts at just \$2.99 / month, and is well worth it.





## Users

If your account is the easiest way for someone to get access to your BigCommerce store, then the second easiest would be the accounts that you've created. Each user in BigCommerce should be given their own account. Never, ever share a password and use a common login.

For each user that you create, make sure you only give them the minimum permission that they need to do their job.

For example, if you create an account for someone to manage orders, only give them the permission to see and edit orders. Don't give them permission to modify products, or other items in your store.

When you create a user, you also have the option to give them "Webdav" access. Webdav is a way for users to interact with your site and access it using something other than their web browser. You should never enable Webdav access for a user account - instead you should create a separate webdav access user for each user who needs webdav access, and have them use that username and password when using webdav.

### Create a User Account

A user is someone who has access to the administration area of your store. Each user account also has its own customizable access permissions, which you can setup below.

#### User Details

Email

Status  ⓘ

#### Permissions

Permissions allow you to restrict which areas of the administration area this user can access. For more information on permissions please see [this article](#).

User Role  ⓘ

Sales Staff Permissions

- Manage Orders
- Edit Orders
- Add Orders



## Apps

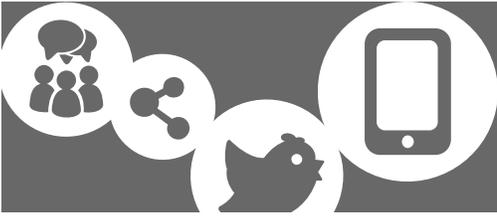
Apps extend the functionality of your store with additional features and functionality that aren't available from BigCommerce natively. However, as with all integrations, you need to be very careful about the apps that you install in your store.

To understand the risk with apps, you need to understand that many apps require access to your store. When you install an app, you can see what access it gets to your store. Here's the MailChimp app for example:

A screenshot of a BigCommerce app access request interface. On the left, the text reads: "MailChimp is requesting access to your BigCommerce store". Below this, it says "By installing this app, MailChimp will be able to:" followed by a list of permissions with green checkmarks: "View site content", "View customer information", "View and modify basic store information", "View general store information and settings", "View marketing information", "View orders", "View products", and "View your basic information (name, email)". Below the list, it says "MailChimp will not be able to:" followed by a red X and "Access your password". On the right, there is a white box containing the MailChimp logo and a blue "Confirm" button. Below the button, a small line of text reads: "By clicking 'Confirm', you agree to the BigCommerce terms of service and the MailChimp privacy policy."

From this you can see that it's requesting the ability to "View" your store information.

Here's our app, Rewind, which needs "Write" access to your store information:



## Apps

Rewind - Backups for BigCommerce is requesting to update its access to your BigCommerce store.

If you agree, the following permissions will be added:

- ✓ View order transactions

For reference, Rewind - Backups for BigCommerce currently has the following permissions:

- ✓ View and modify site content
- ✓ View and modify customer information
- ✓ Log in any of your customers to your storefront
- ✓ View and modify basic store information
- ✓ View general store information and settings
- ✓ View and modify marketing information
- ✓ View and modify orders
- ✓ View and modify products
- ✓ View your basic information (name, email)

Rewind - Backups for BigCommerce will not be able to:

- ✗ Access your password



Notice that the permissions are “View and modify” rather than just “View”.

You need to be cautious about installing apps that can view and modify your store content. They have the ability to modify or delete items in your store.

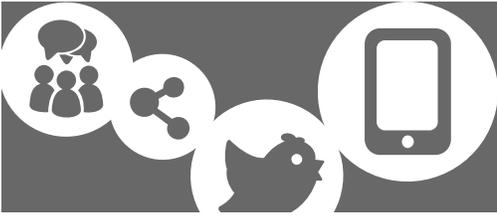
Only you can determine whether the risk of installing an app is worth the benefit. Here are a few things to look at to determine whether an app is trustworthy:

How many reviews do they have? An app with more 5-star reviews can be trusted more than an app with only 1 or 2.

Is the app developed by a company or a single developer?

Does the company have a 1-800 number that you can call?

Does the company publish their contact information?



## Backups

Lastly, despite all your best efforts and security practices, sometimes stuff happens. Employees make mistakes. Apps that have been reliable experience problems.

At the end of the day, your best option is to have a backup of your store. There are apps, like Rewind, which automate backups of BigCommerce, or you can export some of the data manually.

When you export your data manually in CSV format, you'll notice that some of the columns contain multiple pieces of data.

For example, the Category Details and Images columns can both contain multiple items in one cell. Be sure you understand the format of them before modifying any content in them.

It's important to know that when a product is deleted, all the images associated with the product are deleted as well. If you're relying on manually exporting a CSV file, you'll need to save your product images separately.

If you use [Rewind](#) to [backup your BigCommerce store](#), it will automatically save each of your product images, and restore them if required.

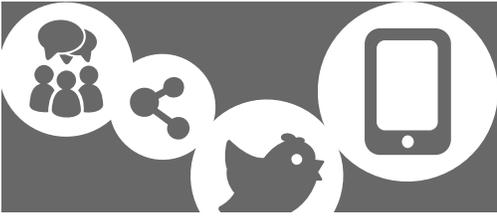
# Rewind - Backups for BigCommerce

Automatic backups to protect your BigCommerce store.

Home

Vault

## Details



## Checklist

- Changed password to something secure
- Signed up for a password manager to manage my passwords
- Created user accounts for everyone who has access to my store
- Limited their access to only what they need
- Reviewed all the apps in my store and removed ones I no longer needed
- Backed up my store