

"Rewind is a lifesaver, I wouldn't want to be without it"

—Jim Smith, Matriarch Perfumes


The Ultimate Guide to

Securing Your Ecommerce Store





Contents

- 1** | Tip 1: Generate an unhackable password
 - 3** | Tip 2: Be stringent around user permissions
 - 5** | Tip 3: Be aware of the permissions
you're granting to apps
 - 8** | Tip 4: Setup two-step authentication
and keep the bad guys out
 - 12** | Tip 5: Back. It. Up. So you can hit undo
 - 15** | Tip 6: Set it and forget it
- 

The ultimate guide to securing your online store

Steps to Protect and Backup Your Ecommerce Store

Your online store is incredibly valuable. Regardless of whether it gets one order or millions of orders, it represents an incredible amount of blood, sweat and tears that needs to be protected. You've spent countless hours perfecting the layout, ensuring your products look great and doing everything you can to give your customers a brilliant experience.

For all these reasons, you'd be devastated if something happened and your site broke – or worse, was hacked.

For all these reasons, you'd be devastated if your site broke – or worse, was hacked.

Yet for many ecommerce store owners, this is your reality. Online stores become inoperable after human error and accidental data deletion, or rogue apps make unwanted changes – in some cases deleting your entire store.

You wouldn't be crazy to wonder why this is a problem.


Surely because it is hosted 'in the cloud' means the customer service team at your ecommerce provider can wave their magic 'undo' wand and revert your store back to what it was?

Unfortunately, this is not the case.

While the ecommerce providers do backup their data, the issue is that your data backups are NOT accessible – not even for a price. So if something goes wrong and you desperately need to hit Ctrl + Z, customer service won't be able to help you.


Without your own backup, your data is unrecoverable and you will be grinding away rebuilding your store.

We feel your pain – the thought of this makes many ecommerce store owners nauseous.



As a business owner, data backup and security should be your top priority. After all, if your site goes away, so too does your income.

In this ebook, we've put together our six most valuable tips to ensure your store is adequately protected from erroneous or malicious harm. We've also included the scoop on the 5-star rated app we personally use and recommend that will ensure you can recover deleted items and undo changes easily.

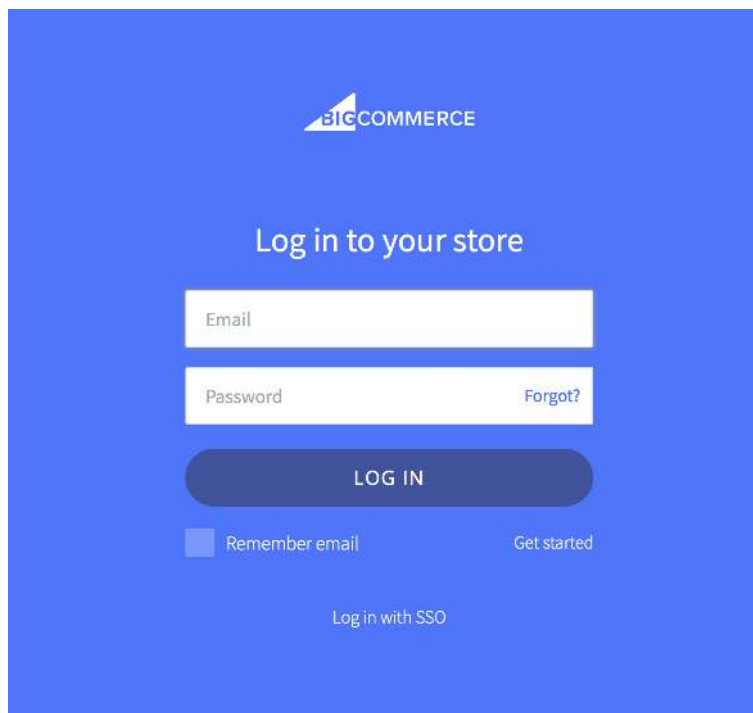


1

Generate an unhackable password

A strong password for your ecommerce store's main administrative account is key to protect your info, your customers info and your online assets. To prevent your main account from being hacked by social engineering, brute force or a dictionary blast, it is imperative that you generate a password following secure password best practices. After all, should someone manage to hack into your main account, they could wreak havoc on your store's appearance and function – not to mention what they could do with access to your customer data.

Your passwords should be so complex that memorizing it should be impossible.

A screenshot of the BigCommerce login interface. The background is a solid blue color. At the top center is the BigCommerce logo, which consists of a white triangle pointing right followed by the text "BIGCOMMERCE" in white. Below the logo, the text "Log in to your store" is centered in white. Underneath this text are two white input fields: the first is labeled "Email" and the second is labeled "Password". To the right of the "Password" field is a link that says "Forgot?". Below the input fields is a large, rounded blue button with the text "LOG IN" in white. Under the "LOG IN" button, there is a checkbox labeled "Remember email" and a link that says "Get started". At the bottom center, there is a link that says "Log in with SSO".

To prevent this, we recommend you create a strong password that has the following characteristics:

- at least 12 characters
- a random mix of uppercase letters, lowercase letters, numbers and symbols
- doesn't contain any names of families, friends or pets
- doesn't contain birth dates, phone numbers, postal codes or other numbers associated to you
- doesn't contain any dictionary words
- is impossible to remember

It is also not advisable to let your web browsers store your passwords (i.e. Chrome, Firefox, Internet Explorer) since all passwords saved can be revealed easily. And because they're so complex, it's going to be unlikely that you can rely on your memory to login easily.

For that reason, we choose to use a password manager to help us minimize the inconvenience of having to reset them and for ease of use – most have a browser extension, web portal and app. 1Password and LastPass are both excellent options to manage your passwords.



Tip #1: Signup for **1Password** or **LastPass**.

Reset all passwords and generate new, secure passwords (based on the above stipulations) for all your logins.

2

Be stringent around user permissions

If hacking into your main user account is the easiest way for someone to get access to your online store, then the second easiest way is via the additional user accounts you've created.

As a rule of thumb, **never, ever share a password or use a common login.** Each user should be given their own account.



Tip #2: Create new user accounts and secure passwords for all other users of your ecommerce store.

< Account

Add staff account

Send invite

Staff account

Give staff access to your store by sending them an invitation. If you're working with a designer, developer, or marketer, find out how to [give collaborator access to your store](#).

First name Last name

Email

☐ This staff account will have full permissions

Select what this staff account can view and edit.

General	Online store
<input type="checkbox"/> Home	<input type="checkbox"/> Themes
<input type="checkbox"/> Orders	<input type="checkbox"/> Blog posts and pages
<input type="checkbox"/> Draft orders	<input type="checkbox"/> Navigation
<input type="checkbox"/> Products	<input type="checkbox"/> Domains
<input type="checkbox"/> Gift cards	
<input type="checkbox"/> Customers	
<input type="checkbox"/> Reports	
<input type="checkbox"/> Dashboards	Point of sale
<input type="checkbox"/> Discounts	<input type="checkbox"/> Locations
<input type="checkbox"/> Apps	
<input type="checkbox"/> Settings	

Cancel Send invite

Secondly, for each user that you create, make sure you give them the minimum permissions that they need to do their job.

For example, if you create an account for someone to manage orders, only give them permission to see and edit orders. Giving them unnecessary permission to modify products or other items in your store increases your risk – whether it be malicious or erroneous.



Tip #3: Login to your ecommerce platform, audit and modify all the permissions of each user ensuring they have the bare minimums of permissions required to do their job.

3

Be aware of the permissions you're granting to apps

Ecommerce platforms make it as simple as possible to start and grow an online business. They include virtually everything you need to get a store up and running. And their APIs have created a huge opportunity for store owners to customize and add additional functionality to their stores via free and premium apps.

On average, each of Shopify's 500,000 users have 3.8 apps installed.

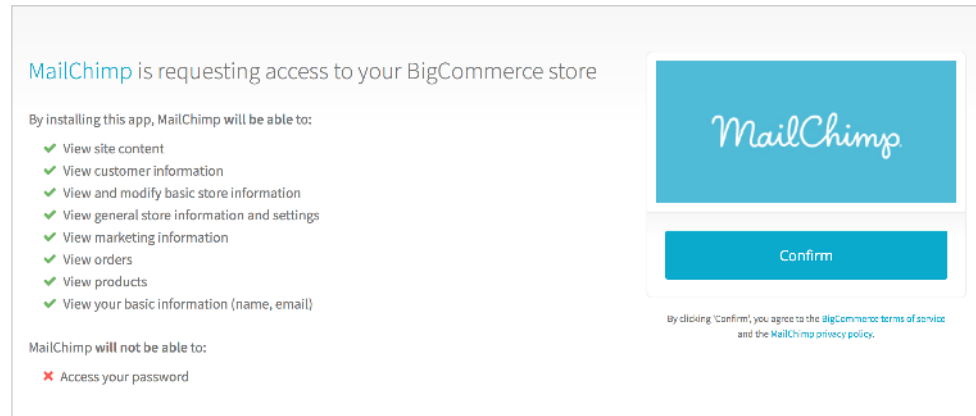
This is however where danger can lie. As with all integrations, you need to be very careful about the security inherent in the apps that you install and grant access to your store.

When you install an app, you are asked to review and confirm what access it requires to your store. The safest type of permissions to grant are 'View' or 'See'. Those with greatest amount of risk are those requesting to 'Manage' or 'Modify' your data.

It doesn't mean that those apps that require permission to manage your data are bad apples. It just means that you are increasing the risk that your data 'could' be manipulated or edited in a manner out of your control. Ensuring you understand the nature of the app's request (is it odd to request this access or does it make sense?) and that you have trust in the developer (check the reviews!) will reduce this risk.

Let's look at an example.

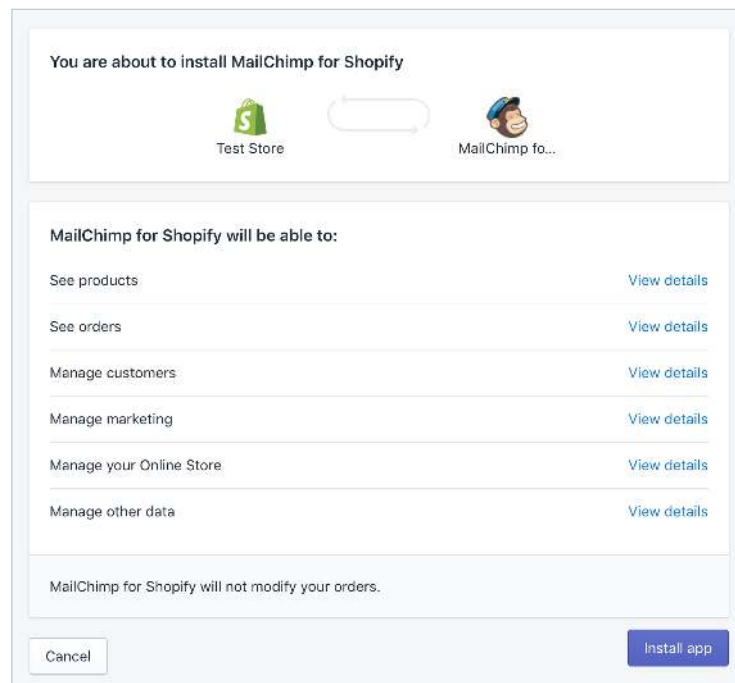
MailChimp Email Marketing app



From this you can see that it's requesting the ability to "View" your store information. Not edit, or manipulate your store data. That makes sense and the app has a significant number of seemingly legit reviews in the app store.

Verdict: Low risk. Safe to install.

Contrast this experience to that with installing this app to the Shopify platform. You'll notice below that the permissions are to "See" and "Manage" rather than just "View".



"Manage" is Shopify's way of saying the app may modify them, and when apps can modify them, that includes accidental deletion.

Verdict: Potential risk. Look into it.

It's for this reason that you need to be cautious about installing apps that can view and modify your store content – you are granting the app the permission to modify or delete items in your store. And if you don't have a backup, then you may be recreating your store from scratch.

In this case, MailChimp is a trusted company, so we've deemed it safe to install and have had no issues whatsoever.

So how is a shop owner to know what apps to trust?



Tip #4: Research, research, research to determine whether the risk of installing an app on your store is worth the benefit.

Here are a few things to determine whether an app is trustworthy:

1. How many reviews do they have?
2. Do they have a 4 or 5-star rating?
3. Is the app developed by a company or a single developer?
4. Does the company have a 1-800 number that you can call?
5. Does the company publish their contact information?

Needless to say, the 750 reviews, 4.5-star rating and past positive experience, were all factored into our decision to install the MailChimp app in our Shopify store. That's not to say we don't have a data backup plan though just in case it was to edit or delete any of the data accidentally – on to that shortly.

The screenshot shows the Shopify App Store interface. At the top is the Shopify logo and navigation links: SUPPORT, HELP CENTER, FORUMS, THEMES, APPS, EXPERTS, and a FREE TRIAL button. Below this is the 'App Store' header with a sub-header 'Powerful new features, services and plugins for your Shopify store'. There are links for 'Sell your own app' and 'Test Store 10034 (log out)'. A filter bar shows 'Category: All', 'Price: All', 'Sort by: Popular', and 'Collections'. A search bar is also present. The main content area displays the 'MailChimp for Shopify' app, developed by MailChimp, with a 4.5-star rating and 758 reviews. A green 'Get' button is visible. Below the app name, there are three bullet points: 'Connect your Shopify store with your MailChimp account (for free)', 'Automatically add customers and their purchase data to MailChimp', and 'Create targeted abandoned cart, email marketing, win-back, and post-purchase email campaigns based on buying behavior'. On the right, a 'Price' section shows a 'Custom' price option and a description of the app's features and pricing plans.

4

Setup two-step authentication and keep the bad guys out

Even with all the advice we've given you above, it's STILL possible that someone could steal your password. They could lock you out of your store, and do something terrible like

- Delete all your products, customers and orders
- Go through your customer's personal information
- Add malicious code to your theme that visitors will download
- Pretend to be you and send unwarranted or hurtful emails to your contacts
- Delete your shop permanently!

Two-step authentication is an extra layer of security designed to ensure you are the only person who can access your account. Even if someone steals your password, they'll still need your phone or verification code to get into your account.

It works by generating a unique code on your mobile device, requiring you to enter that code after you've entered your password. 1Password, which we mentioned above, also supports 2-factor authentication without needing a mobile device, which makes it much more convenient.



Tip #5: Make your account even stronger and set up two-step authentication for all user accounts.

Steps to setting up two-step authentication for Shopify

1. To setup two-step authentication, you'll need to download the 1Password (our preference) or the Google Authenticator app.
2. Login to your Shopify account, click on your name in the top right-hand corner, and select Your Profile.



WAYS TO SELL ▾ PRICING BLOGS RESOURCES ▾

A screenshot of the Shopify login page. The background is dark grey. In the center is a white rounded rectangle containing the login form. At the top of the form, it says 'Log in to your Shopify store' in bold. Below this are three input fields: 'Store address' with '.myshopify.com' pre-filled, 'Email address', and 'Password' with a 'Forgot?' link to its right. Below the fields is a large blue 'Log in' button. At the bottom of the form is a checkbox labeled 'Remember me' which is checked.

3. Scroll to the section for two-step authentication. Click on Enable Two-Step Authentication. You'll be prompted to enter your password to continue.

A screenshot of a notification box for two-step authentication. On the left, under the heading 'Two-step authentication', is a paragraph explaining the feature. On the right, a white box with a grey border contains the message 'You have not enabled two-step authentication.' followed by a paragraph explaining the security benefits. At the bottom of this box is a button labeled 'Enable two-step authentication'.

You can choose to receive codes either by SMS message or using the Authenticator app.

Enable Two-Step Authentication

SELECT A TWO-STEP AUTHENTICATION METHOD

Choose how you want to receive the special code you'll use to authenticate your account.
[Learn more about Shopify-supported delivery methods.](#)

SMS Delivery

☐ Authentication codes are sent to your mobile device using SMS messaging.

Authenticator App

☐ Authentication codes are generated by an application on your mobile device.

Cancel

Next

4. If you select to use the SMS Delivery method of two-step Authentication, enter in your mobile phone number. In a few seconds, you'll receive a unique six-digit code by SMS. Enter that unique code into the field on your screen. Two-step authentication is now enabled on your account.

Enable Two-Step Authentication

1. Add mobile phone number

Enter the phone number of the mobile device you'd like your authentication codes sent to each time you log in.

Country code

Canada +1

Phone number

Send code

2. Enter the six-digit code received on your mobile phone

Cancel

Confirm

5. If you select to use Authenticator App method of two-step Authentication, you'll be asked to scan a code. You can scan that code using the Google Authenticator app, or 1Password.


Enable Two-Step Authentication

1. Install an authenticator app

To generate the codes needed to log in to your account, please install a Shopify-supported authenticator app on your mobile device. [Learn more about supported apps](#)

2. Configure the app

Open the authenticator app on your mobile device and scan the QR Code.
Can't scan the QR Code? Configure your app with this key: [Click here to display key](#)



3. Enter the six-digit code generated by the app

Cancel

Confirm

6. Once you've scanned the code, the Authenticator app or 1Password will generate a unique six digit code. Enter the code generated by the app, and click on confirm. Two-step authentication is now enabled on your account.



5

Back. It. Up. So you can hit undo

You've gone to all the trouble to ensure no bad guys are going to break in and play havoc with your shop. Kudos to you! But what about human error? Despite all your best efforts and security practices, people make mistakes. Apps that have been reliable in the past experience problems.

Not having a daily backup of your store, is like having your house burn down without insurance. You'd have to start all over again.

But surely I can just contact customer service and get them to recover my data?

No.

Revert it back to what it was yesterday?

Nope, sorry.

Gulp.

We know. This is a shocking realization for many store owners who assume they have access to their backups if they have an issue.

Rest assured these platforms are doing a great job at keeping your data secure, and they'll also do their best to walk you through some manual steps to rebuild your content. However you can't rely on them should you need to restore your site, undo a change or revert back to a previous iteration.

Some store owners choose to backup manually – which involves saving your theme, and products manually to a hard drive, or by exporting everything to CSV. It's important to know that when a product is deleted, all the images associated with the product are deleted as well. So if you're relying on manually exporting a CSV file, you need to save your product images separately.

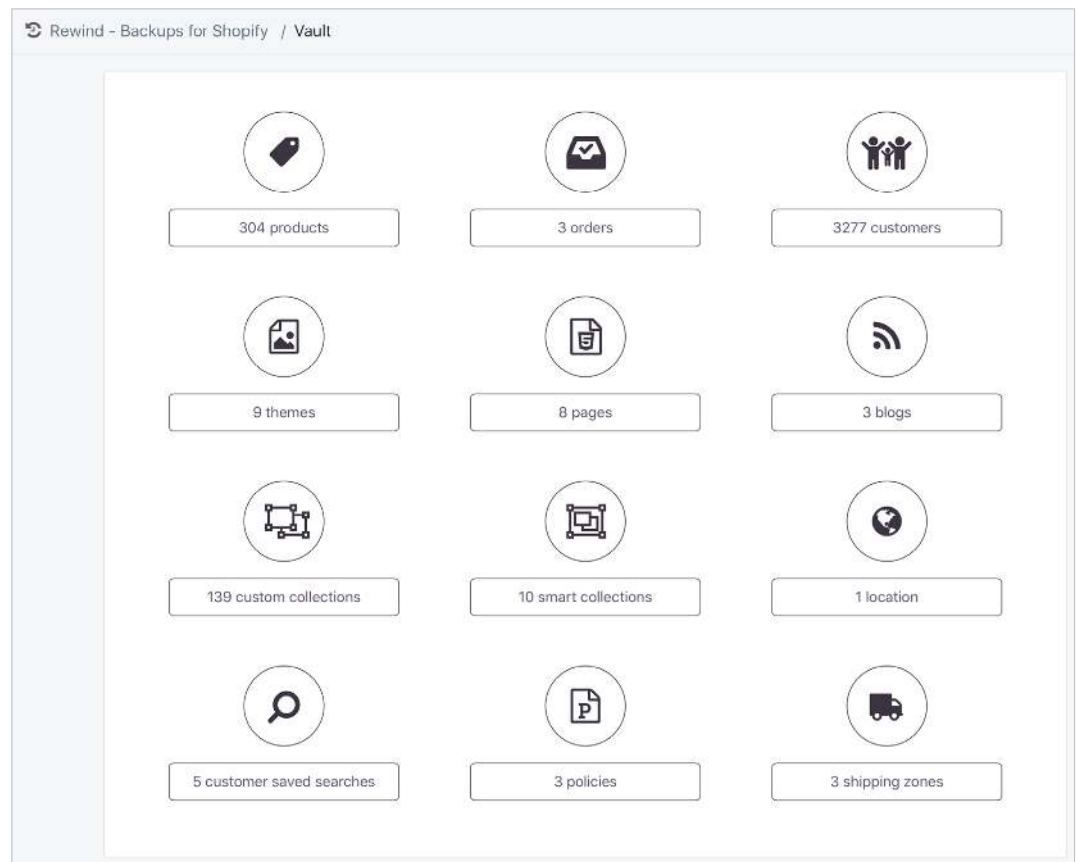
This is definitely time-consuming and a hassle for store owners trying to grow their business. It's an even bigger hassle to restore from.

Your best option is to use an app to automatically backup your store and restore it when required with an automatic backup application – like **Rewind**.

The screenshot shows the Shopify App Store interface. At the top is the Shopify logo and navigation links: SUPPORT, HELP CENTER, FORUMS, THEMES, APPS, EXPERTS, and a FREE TRIAL button. Below this is the 'App Store' header with a sub-header 'Powerful new features, services and plugins for your Shopify store'. A search bar and filters for Category (All), Price (All), and Sort by (Popular) are visible. The main content area features the 'Rewind - Backups for Shopify' app by Rewind, which has 296 reviews. The app's interface is shown, displaying a dashboard with icons for Products, Collections, Themes, Customers, Blogs, and Pages. A list of backup items is visible, including 'All Product Details', 'Only Product Images', 'All Custom Collections', 'All Smart Collections', 'All Themes and Files', 'All Customers', 'All Blogs and Articles', and 'All Pages'. To the right of the app preview, there is a 'Get' button, pricing information ('From \$5.00 / month'), a 'Free Trial' of 7 days, and contact information for support and sales. Below the app preview, there are three bullet points highlighting key features: restoring deleted items, importing CSV files or syncing inventory, and automatic backups of all store data. A section titled 'With one click you get a complete, automated backup system that keeps your Shopify store safe.' is also present, followed by a brief description of the app's functionality.

The app takes a snapshot of all the data on your store and saves it by date in the Rewind Vault. It saves everything – products and product images, customers, orders, blogs, blog posts, comments, collections, themes and all the theme files.

To restore your store, you simply pick the date that had the version you want, and hit restore. It's a one-click process, and you can choose flexible restorations (just restoring one item, a collection of items, or the whole store).



This flexibility gives you an enormous amount of control over your store – and over your time. You can rest easy, knowing that if something goes awry, it's going to be a matter of moments to fix it, rather than hours or days.



Tip #6: Check out Rewind's **perfect 5-star rating** on the **Shopify** and **BigCommerce app** stores, and give their customer service a whirl with a free 7-day trial.



Set it and forget it.

In this e-book we've given you some tips and tricks on ways to secure your user accounts and your online store in order to minimize risk from malicious attempts to break your data, human error or rogue apps.

Remember however, **your security is only as good as your weakest point, so implementing just one or two of these recommendations may not be enough.**

The best insurance policy is to ensure that you have access to a complete backup of your site. That way, if something does happen, you'll have the data, images and files available, and can recover super quickly.

Get peace of mind. Follow the recommendations above and you'll save days of repeat work, save lost sales, and save yourself from an avoidable stress.



Tip #7: Give **Rewind** a whirl and get peace-of-mind that everything is backed-up and most importantly, restorable. Signup here for a **free Shopify trial here**, or **free BigCommerce trial here**.

The Ultimate Guide to

Securing Your Ecommerce Store

Visit us at rewind.io