rewind

3 Simple Ways to Protect Your Online Store

A Rewind Webinar for Ecommerce Merchants

Hey everyone and welcome to How to protect your online store. Today we're going to cover 3 simple ways to secure your BigCommerce or Shopify Store.

My name is Emma Hyde, and I am a Product Marketing Manager with Rewind. To give you a quick introduction to Rewind, we are a fully automated backup and restore app for your online store.

About Rewind

- Rewind is a tool that protects your BigCommerce store.
- Automatically backs up all of the essential data in your Shopify or BigCommerce store and makes it easy to restore that information in minutes.
- We are a leading backup app for Shopify, BigCommerce, QuickBooks Online, and GitHub.
- We were founded in 2015 and are based out of Canada's capital city, Ottawa with employees spread across the country.

Rewind works with global brands around the world to power their backups and make sure their data is secure. We have more than a thousand 5-star reviews across all of our platforms, including BigCommerce, Shopify, QuickBooks, GitHub, and most recently, Trello, the productivity and organizational tool. We are constantly working to add more platforms to our suite of backup solutions.

Let's look at the 3 best ways to protect your ecommerce store.

2FA

Most people in the digital world have seen some kind of tips on password security, but not all of us are familiar with 2FA. Two-factor authentication helps ensure that you're protected by adding a second layer of security to your online data.

Your password is something you know, which means it's something that can be guessed or stolen. 2FA is something you have, e.g., your phone. The combination of the two is what helps to keep your data secure. So why do you need it?

Passwords are compromised every day. Just a few weeks ago, Facebook and LinkedIn were part of yet another data scraping exercise. If you're interested in seeing whether or not your email address or passwords have been disclosed in a data breach, there are sites like "Have I been Pwned" that will search for your data in the lists of recent breaches and let you know if you've been compromised. If you have been compromised, the best thing to do is to change your passwords and set up 2FA.

There are different ways to set up two-factor authentication. For example, by default, BigCommerce requires users to set up 2FA with their email. Other tools might send an SMS text message to your phone.

The most secure system is through an authenticator app. Your email can still be broken into, especially when a lot of us are guilty of using the same password for multiple sites. Dedicated hackers have also been known to pull some funny business and temporarily steal your phone number to get access codes.

But with an app, the code is only available on your device. No one can steal it, and only you have access to it.

To set it up with Shopify, go to your name in the top right corner in your Admin portal and select "Manage Account." From there, on the left click "Security" and in that tab you'll be able to set up "Two step authentication."

BigCommerce just released the option to set up 2FA with authy, and I encourage everyone to look into it for their store, as well as any other tools. From your control center, just go to My Profile > Additional Authentication.

Password Security

Modern passwords are often hard to remember, but easy to crack. Every site requires 8 characters, one number, one capital letter, one lower case letter, a special character, your first born child. It's too much, and for what?

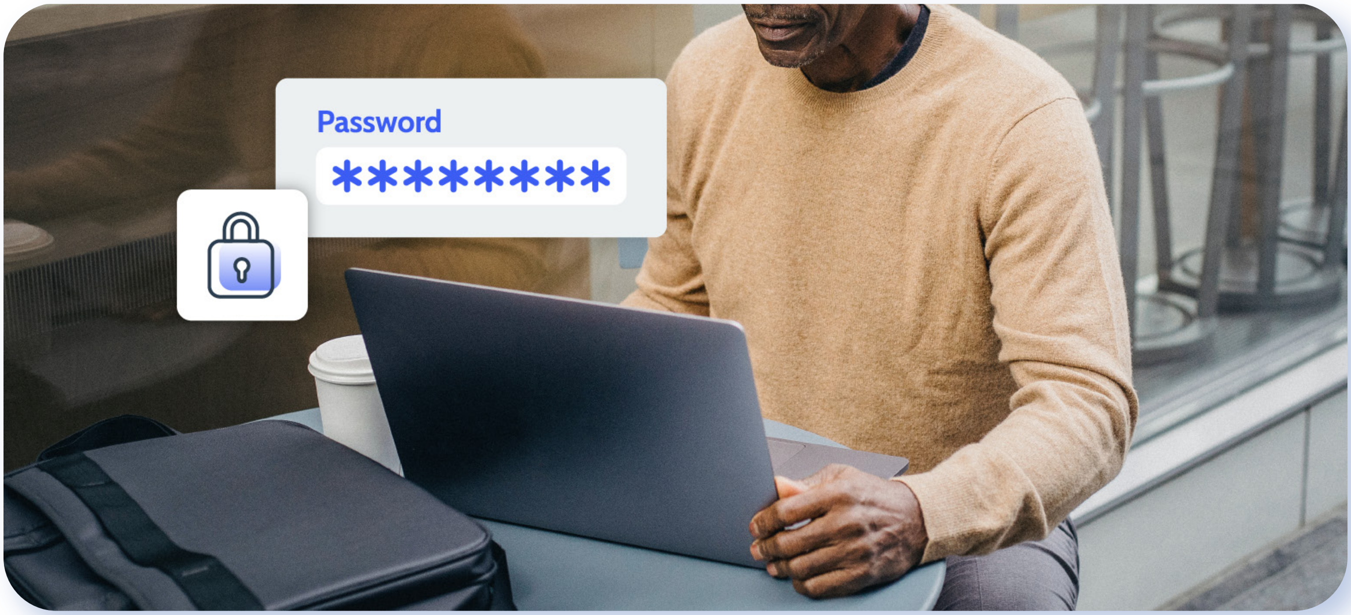
When we think of people hacking our passwords, we as humans often assume that they're guessing the password, but that's not the case. Every password is essentially the code to a combination lock.

Combination locks get infinitely more difficult to crack the longer the number. So for a lock with 4 numbers, there are 10,000 possible combinations. For a lock with 5 numbers, there are 100,000 possible combinations.

If a hacker is trying to guess a password, they'll do it through the use of scripts and programs. Those scripts and programs can run through all of the possibilities quickly and efficiently. Because of this, the best thing you can do is use a longer password. The longer the password, the more combinations, the less likely you are to be hacked.

One of the easiest ways to lengthen your passwords is to use a passphrase rather than a password. But if you're anything like me, you have passwords to more sites than you can count, and that still leaves you with the problem of trying to remember your passwords (and username in some cases) for every single one of those.

That's where password managers come in. There are lots of options, they all have their perks, and it's easy to find a free one. Last-Pass, One Password, and Bitwarden are all great options. Or, if you live and breathe the Apple ecosystem, their Keychain feature is a great one. All password managers keep a collection of long, complex, and secure passwords for all the sites that have been saved in their vaults; users only have to remember a single, secure Master Password to log into each site.



User Roles & Permissions

Let's talk about managing who and what has access to your store, i.e. your user access policy.

If you have a team of people, you want to make sure they're able to do their job quickly and efficiently. But don't forget to regularly audit the list of users on your store.

Life happens, people quit, agencies are brought on and phased out and it's easy to forget who had access to what tools.
More often than not, malicious or targeted attacks come from unhappy employees that are looking to get back at the business for one reason or another. Every person that has access to your BigCommerce store has the power to affect your business.

And that extends to current employees and team members. We all need certain tools and permissions to do our jobs. Most of us are so careful when we're hiring and we do our best to choose the right people for the job. But it's easy to forget that even the best people make mistakes. We're human. Sometimes we delete a product or change the wrong photo on a listing.

It's best for everyone when your user permissions match your team's job description. That way, they are only able to make the mistakes within the parameters of their responsibilities.

The last thing you want is your staff accidentally deleting essential information by mistake when you have to be the person to clean up the mess.

Third-Party Apps

Additional surface area that's open for attacks is third-party apps. Our customer support team has seen a number of cases where a bug is introduced into an installed app, only to accidentally delete an entire product catalog.

One of the best parts of BigCommerce is the flexibility to connect to a variety of tools through their headless API. It's a great system, but it does come with risks.

If you have external tools with separate login credentials, make sure they're secure. Every app you connect to your store has visibility into some part of your business, and the last thing you want is for your apps to turn against you.

How can you minimize your risks? Be very selective. Read reviews. Before you install anything on your store, make sure you do your due diligence. Look out for reviews or online forums discussing any problems people have had with the app. Hunt down those one-star reviews and try to understand what people are upset about and if their setup is similar to yours.

Once you've decided that an app is essential to your business, make sure you always have the latest version installed.

The vast majority of apps today are connected through the app store, but if you have any custom tools that aren't updated through the cloud, make sure you always have the latest version.

Apps
Search apps by name or category (e.g. productivity, sales)
Apps in The Sandlot (3)
Teamline
The simple project management tool for Slack
Google Calendar
Hubspot
Marketing, sales, customer service and CRM
Donut
Guru
Your integrated knowledge management tool for Slack
App Recommendations
Google Drive
Giphy

Automatic Backups

And now for our favourite security solution, automatic backups!

A lot of us don't think of backups as a security feature, but it really is. It's a safe way to have a clear history of your store. This means you're free to update your products, experiment with new messaging or images, and work with your team without fear of mistakes.

It's important to look for two things in a backup: they should be automatically triggered, and they should be consistent. A good rule of thumb is to use daily backups. Let's be clear: manual backups just don't work in today's world.

Tech has enabled us as individuals and as businesses to move so quickly, and that means that if you're backing up your data manually, you will inevitably fall behind. Whether it's because you run out of storage, or you simply forget to export your CSV file for the day, it's simply not manageable. Not to mention all the time it takes to dig through those old CSV files.

Automatic backups are literally your backup plan when the first two security solutions fail you – they can be used as a magic undo button. It's common for employees to accidentally delete photos, or for a third-party app to delete a product catalogue. With a good backup, you can restore your information in minutes.

And time is money.

Downtime costs money. The faster you can recover from crashes or mistakes, the less money you'll lose.

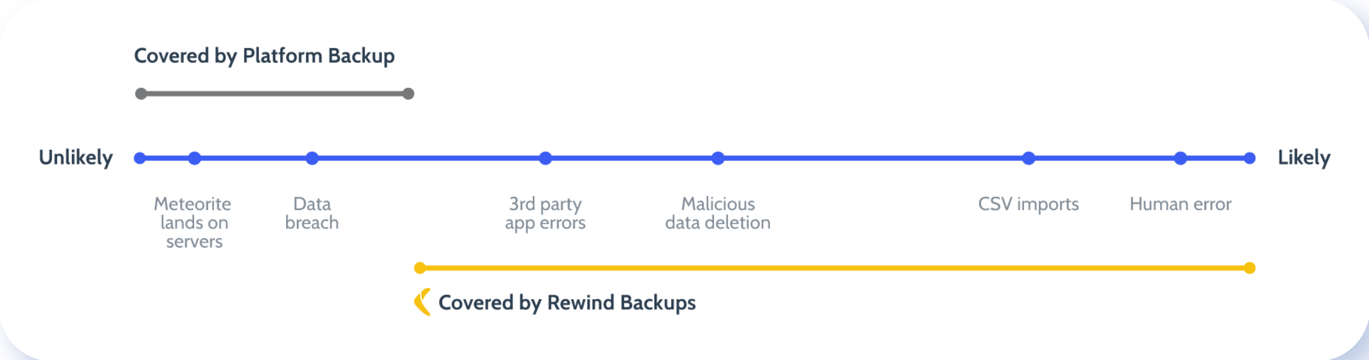
The Shared Responsibility Model

But don't the ecommerce SaaS platforms already back up my data? Sure, they do. But those backups can't be used by individual account holders.

They back up all the stores hosted on their platform at once. If a meteor struck a data centre, you'd be ok — everyone's data could be restored. But restoring individual accounts is like looking for a needle in a field of haystacks.

Think of it this way: You don't own the software, you rent it. You have no physical copy of that data. Because of this "rental" type model, tools like BigCommerce expect you to be the one to take care of your data.

This is called the shared responsibility model. The Shared Responsibility Model is always present. The onus is on you, the user, to understand what data is at risk and how to protect it.



Case Study

The bad news is that disasters are inevitable, and it's on you to clean up the mess when they happen. The good news is Rewind protects you and your business.

Back in 2015, Gymshark faced every ecommerce business's worst nightmare: their store went down on Black Friday. 8 hours of the store being down resulted in close to $143,000 in lost revenue. They signed up for Rewind the next day so that they knew if something went wrong, they had a way to patch things up in minutes.

Get In Touch

Have a question for us? Get in touch at sales@rewind.com.
For more information, visit Backups for BigCommerce.

Contact Us

rewind