rewind

How to Secure Your Ecommerce Store

If websites like Target, Neiman Marcus, and eBay can be hacked, your ecommerce store faces an even greater risk. You know that. That's why you're here—to proactively secure your ecommerce website and the shoppers that keep you growing.

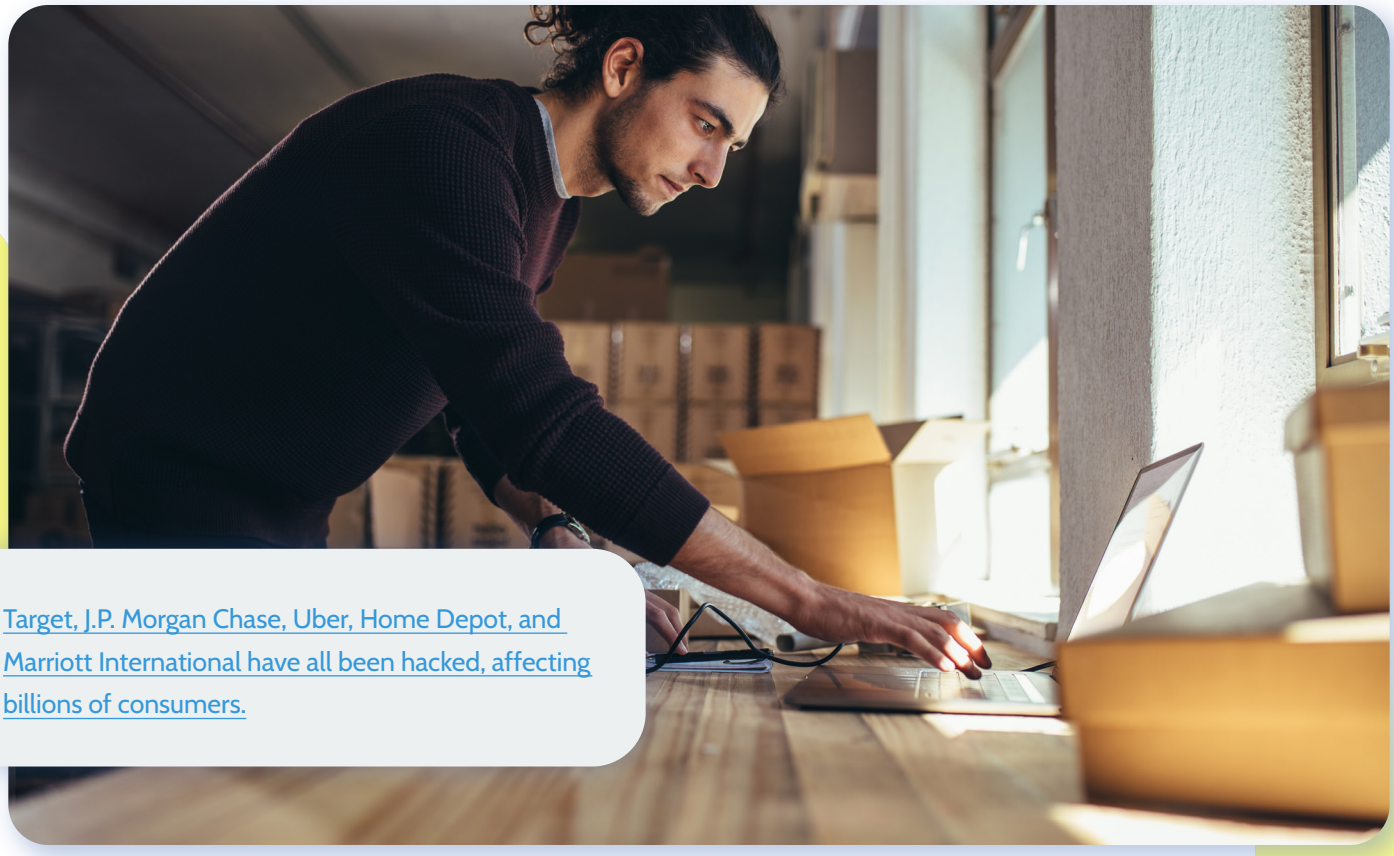
Certainly you don't want to wait until you start hearing from customers that they've purchased something from you and haven't received it, yet you can't find any record of them.

You definitely don't want to be stuck watching your conversion rates plummet because something (or someone) broke your site.

And you definitely don't want to be among the 60% of businesses that shut down after a cyber attack (the average loss from hacking is an insane $4.24 million, $1.23 million for enterprises alone).

WANT TO PROTECT YOUR BUSINESS AND YOUR CUSTOMERS? READ ON TO SEE:

- Exactly how hackers might be able to attack your site (it's probably not what you're thinking)
- How to identify a cyberattack in progress (and what to do about it)
- How to avoid all the spam, spoofing, scams, and hijacking by creating a company culture of security



Target, J.P. Morgan Chase, Uber, Home Depot, and Marriott International have all been hacked, affecting billions of consumers.

Ecommerce Security Issues & How to Secure Your Store Against Them

Most cyberattacks aren't done directly by hackers. They're performed by bots (like the destructive Mirai botnet that breached one of the largest controllers of the Internet's Domain Name Service, Dyn).

That simple fact means that more cyber attacks happen every day than most of us can imagine. After all, bots don't sleep, eat, or take breaks, making the scale of modern cyberattacks staggering.

We're talking 80-90% of your ecommerce site logins being completely automated by bots. One large retailer noticed over 10,000 login attempts from just 1,000 IP addresses.

That points to one of the largest potential weaknesses on your website, and where most attacks take place: at login.

Issue #1: Login & Weak Passwords

Most of us aren't very good at creating or keeping passwords. Mike Potter, co-founder and CEO of Rewind, has a witticism that's applicable here: "If you can remember any of your passwords, they aren't secure enough".

We write them on sticky notes and post them around the rim of our computers. We auto-save them to our browsers. We use the same password for 10 different accounts because we can never remember them, and we never update them.

For the most part, websites will let you try again and again and again until you find the right login.

While Shopify and BigCommerce do limit the amount of login attempts during a session, this is easily circumvented by using different IP addresses. It's a perfect opportunity for bots. They'll just keep trying until they get it right.

And since most passwords are rather simple, it often doesn't take the bot very long. To illustrate just how easy to crack popular passwords are, consider NordPass's top three most commonly used passwords: "123456", "123456789", and "12345".

Solution: Utilize Password Managers & Focus on Password Health

WHAT IS A PASSWORD MANAGER?

Instead of attempting to come up with a unique and random password for each site you visit, you can utilize a Password Manager to generate and remember your passwords for you. After installing, choose a secure passphrase (more on those below) to secure all of your passwords.

HOW DO PASSWORD MANAGERS PREVENT ATTACKS?

Unicode attacks, or script spoofing, is a really challenging problem right now and one of the most common types of attacks ecommerce stores see. What they look like:

Instead of Facebook.com, your customers might see FAcebook.com, FacebOok.com, Facebook.co. Or, for companies that have an L in their title, might show up as an I in this kind of spoofing attack.

Some hackers may use this as a way to open a script and alter something on your site, such as installing malware.

Another way hackers might use a Unicode attack is to create false websites that look exactly like the original, but are designed simply to steal information and passwords from employees and customers.

Things like password managers help you deal with this by barring you from entering a password into a website that doesn't check out. After all, your password manager has a saved password for *Facebook.com*, not *FacebOok.com* or *Facebook.co*. If the URL doesn't match the site the password is meant for, it'll simply say "no results found" when you go to login.

As for good password health:

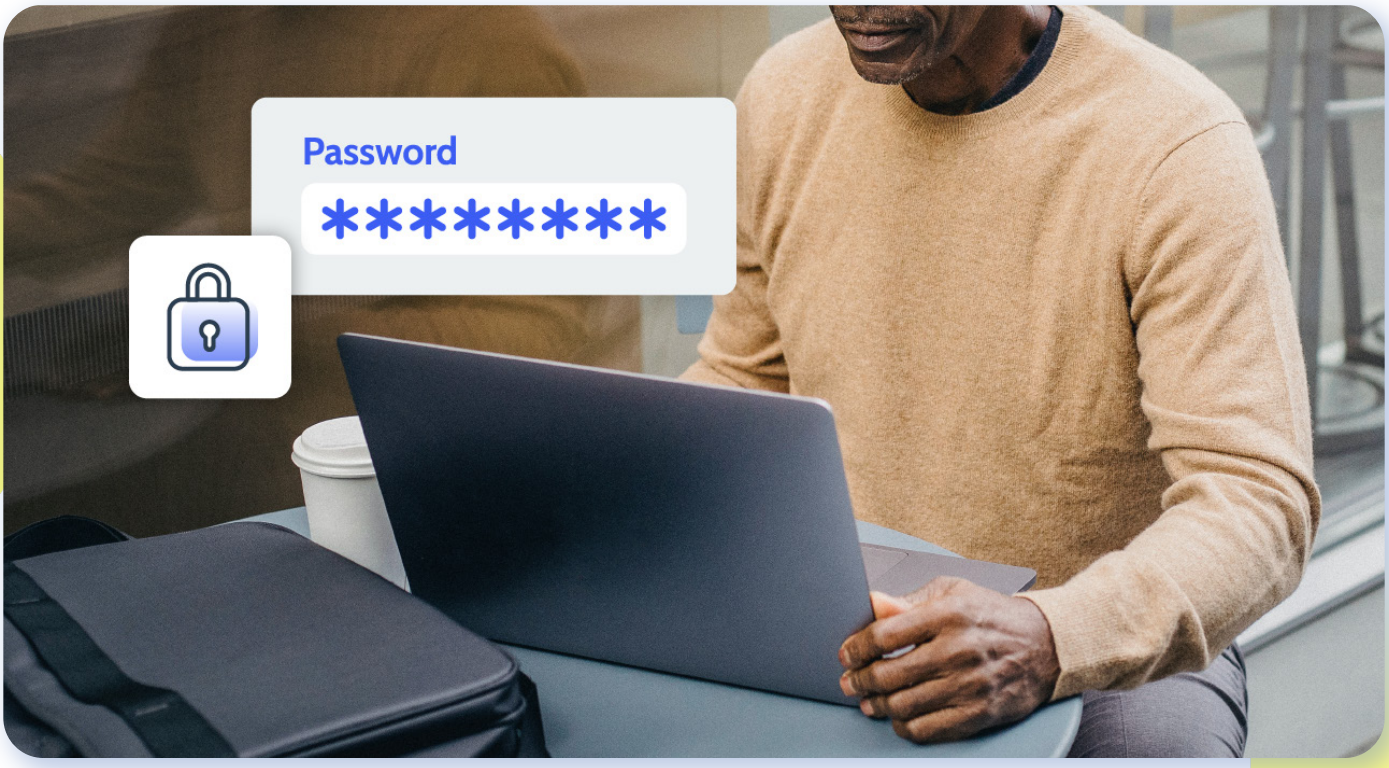
Every company should add password managers to their cyber security policies, but what's challenging about password enforcement in the workplace is it can be a hard thing to balance.

Requiring password changes every 3 weeks isn't recommended, as employees are likely to simply add a number to the end of an existing password because they can't remember it otherwise. Or, they'll come up with passwords they can't remember and have to write them down - which just isn't secure at all, since everyone can see them.

Instead, to create strong passwords your employees should:

- Pick a phrase or rhyme or even a sentence in a random book (known as a passphrase). This longer password should be used as your master password for a password manager, which can generate truly random and secure passwords for you.
- Never use the same password for more than one site
- Use a password manager to keep track of their passwords
- Install 2-step or multi-factor authentication

It's also no longer recommended to change your passwords regularly. Rotate only if you think there's been an attack or you're vulnerable to one. You can always check if your credentials have been leaked or scraped at HaveIBeenPwned.com, a running list of all emails, phone numbers, and passwords that have been compromised or breached.



Issue #2: Your Employees Work Remotely

It likely comes as no surprise that ecommerce businesses with remote workers face a higher risk of security breaches. The cost of that vulnerability is also much higher ($1.07 million higher) than ecommerce stores without remote workers.

THE REASON IT'S SUCH A RISK?

It largely comes down to passwords and credentials.

Compromised credentials are the most common initial attack vector and cause of most security breaches, accounting for 20 of all breaches. It's common because employees use their passwords for too long, share it with other sites or other employees, and use easy-to-hack passwords.

WHY IS IT WORSE FOR REMOTE EMPLOYEES?

In an office setting, you have the ability to update systems all at once because they're all on the same network. Remote employees often use their own laptops. Worse, they often work on the go, in cafes and coworking offices, or in various locations while traveling.

This means they're often operating networks that are far less secure and open to the public – unless they're using a VPN, a virtual private network.

Solution: Every Remote Worker Should Have a VPN & Cybersecurity Training

COVID has really changed how a lot of us work and how a lot of companies function. There's greater use of co-working spaces and cafes, and there are far more international employees working for US domestic companies.

Requiring password changes every 3 weeks isn't recommended, as employees are likely to simply add a number to the end of an existing password because they can't remember it otherwise. Or, they'll come up with passwords they can't remember and have to write them down - which just isn't secure at all, since everyone can see them.

Anyone working outside of your network should have a VPN, ideally a company VPN that still allows you to enforce your security policies. A VPN creates a private network, even while working in public spaces and on public networks. It makes you and your employees far less vulnerable to malware and viruses. VPNs can even work on mobile devices, which is necessary for those consistently traveling while working.

Cybersecurity Training

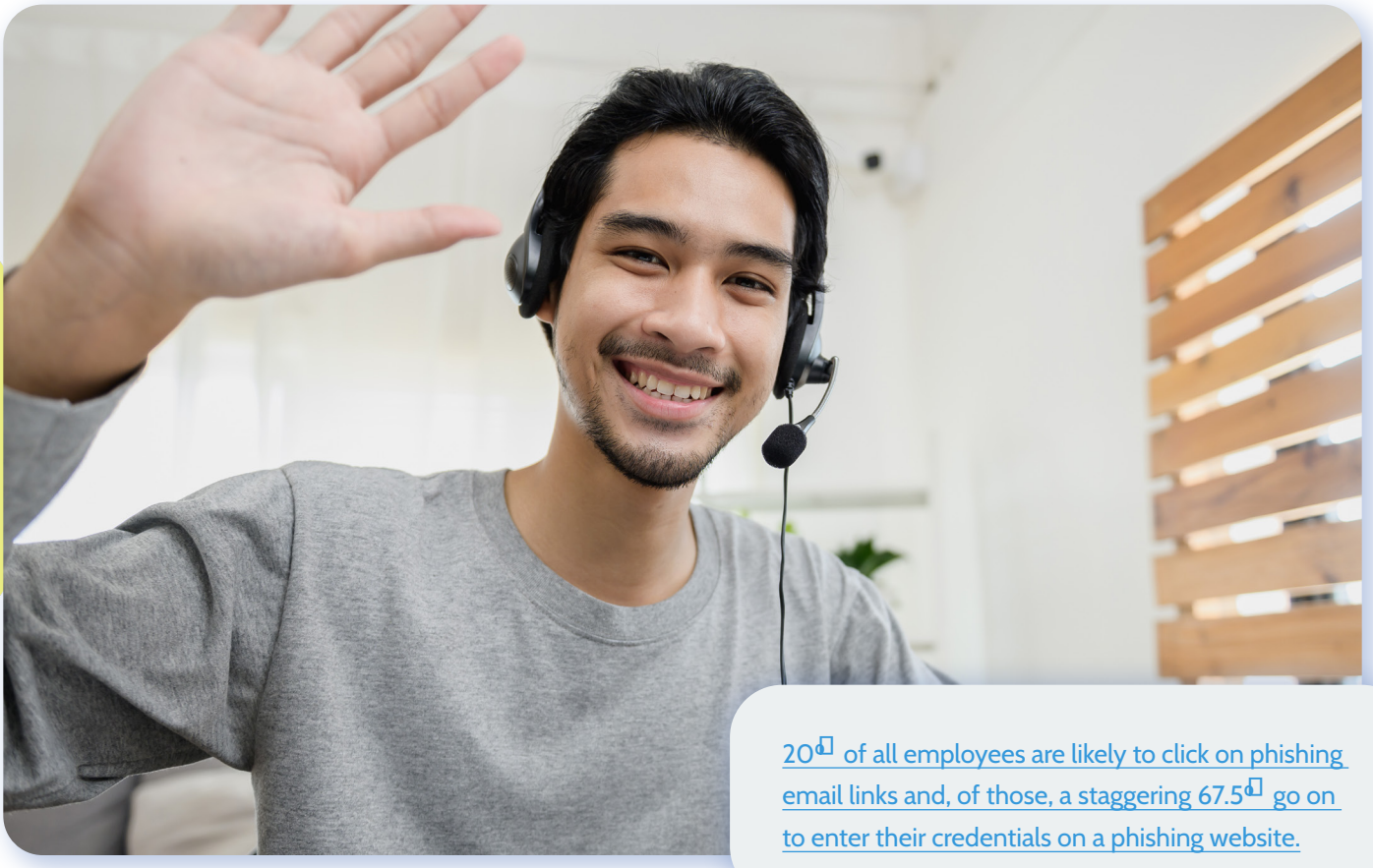
It doesn't have to be anything comprehensive, but if your workers are remote, they need to have some understanding of how vulnerable they are.

Simple mistakes that increase their vulnerability include:

- Leaving their laptop open while they step away for a call
- Using biometric locks instead of pins and passwords
- Using an Apple Watch to unlock a computer

Things like face logins are often easy to access and were once as simple as using a photo of the laptop owner. And just like a car's key fob, hackers can simply replicate your Apple watch signal or even enhance it to gain access to a computer.

So, training employees to lock their computers in a drawer each time they leave it, even for a few minutes (most coworking spaces have drawers with locks), is essential. As is ensuring they understand password safety and have the right software on their computers such as JAMF and a password manager.



20% of all employees are likely to click on phishing email links and, of those, a staggering 67.5% go on to enter their credentials on a phishing website.

Issue #3: You're Not Monitoring Your Shopify and BigCommerce Apps

You give a lot of permissions to apps you install on your ecommerce site. Maybe these permissions seem rather superficial, and at first maybe they are.

The problem with apps often occurs when you update them. It's really challenging to see who's created the app—whether it's a solopreneur or a large company—and to know whether or not you can trust them. At first it may seem that you can, but when you update the app, or the app changes to a new owner, that is when something nefarious may happen.

Daniel Sim, General Manager Commerce at Rewind, shares what this kind of attack looks like:

"We had one really suspicious case come into support. We looked and found that the app had installed one of these scripts, to skim the credit card details. And the interesting thing was, it wasn't when the app was initially installed, it was during an update that the malicious code was added.

Once you've given the app permission to update your site, it can choose when it does that.... This attack was sophisticated enough that it would only enable itself for a very short period of time, just enough to do its nefarious stuff, and then switch itself off.

That way, it was able to avoid detection. We went into the store and looked into the source code, and we couldn't find anything suspicious. But luckily, we were able to catch it in the act when we saw that it was pinging off all of the customers' details to this other server..."

While this is an extreme example, poorly configured or buggy apps can wreak havoc on ecommerce data. Once an app is given read and write permissions, it can edit, add, alter, or even delete your data.

Solution: Check Your Ecommerce Store Web Applications

When you add a web application to your ecommerce store, a window will pop up on the screen that says you're giving permission for the app to do or access X, Y, Z.

But those screens don't always tell the whole story. Sometimes they're really gaining access to all of your product data, and it could mean the app could wipe out your entire product catalog.

The solution:

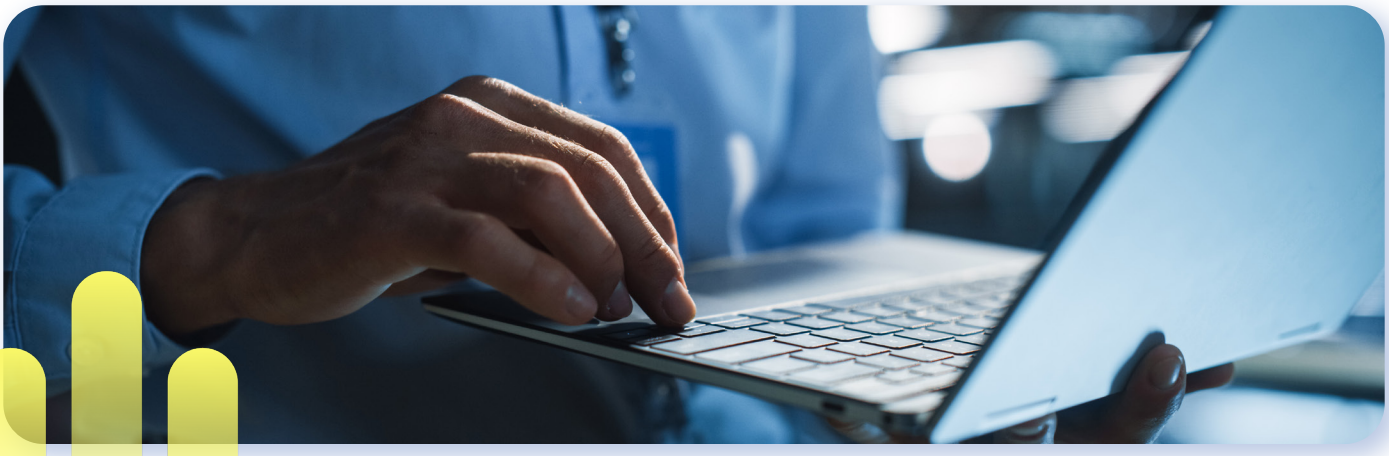
"Not all merchants think about it, but these apps can be from a bad actor or a solo developer. Or, they can be from a huge organization," says Daniel Sim. "A lot of the time, it's very, very hard to know. So something I'd recommend to merchants is to really understand who is behind the app that you're installing."

Your best option is to learn a bit more about the company:

- [ ] Are there comments about the brand online?
- [ ] Do they have updated and complete help documentation?
- [ ] How many other stores have downloaded the app?
- [ ] Does the app have a website with contact information?
- [ ] Is the app developed by a single individual or a larger company?

Essentially, does it look like a kosher company with people behind it, because you're giving them a lot of access to your stored data.

Check up on these apps regularly to see if they've changed hands. Occasionally this may happen, but you should gain the same understanding of this new company, as they may change permissions and access.



Issue #4: Other Attacks You're Vulnerable To

Ecommerce sites (and really all sites on the web) are vulnerable to these types of attacks:

- **SQL injections** attacks your backend database by injecting malicious code into your site script.
- **Cross-site scripting** injects malicious code through vulnerabilities in your web applications that are then executed by users.
- **Malware infections** are all the ransomware, spyware, adware, and other programs that perform malicious actions to cause damage or retrieve information from systems and networks.
- **Distributed Denial of Service (DDoS or DoS)** overloads your network with massive amounts of information to crash the network.
- **Brute force attacks** are when attackers simply try every possible character combination until it matches a valid set of credentials.
- **Phishing** attempts are fake emails or messages intended to retrieve sensitive or personal information, or just to trick the user into performing an action that isn't in their best interest (for example, transferring money to "Bill Gates").

It's a lot to counteract, but most self-hosted sites such as Shopify or BigCommerce have some of that protection built-in to their systems.

Distributed denial of service (DDoS) or Denial of Service (DoS) attacks tend to be the most common type of scam, present in 90% of the data breaches today. Of these attacks, 36% start with a phishing scam (aka social engineering) and the installation of malware on your network.

Luckily, there are a lot of protections against phishing scams in email systems (like Gmail) today, but every now and then a clever one gets through.

The remainder of attacks are typically brute force (a simple use of stolen credentials).

Solution: Use a Firewall

Most cyberattacks today are automated, which means you can block them with a firewall. They won't do as much for attacks conducted by hackers that are specifically targeting you, but those tend to be rather rare.

If you're using a Shopify or BigCommerce account, many protections are already in place, but you can still enable a firewall like WAF (a web application firewall) from Cloudflare, in addition to protections like rate limiting and robot protection that are built into those hosting platforms.

Other Ecommerce Website Security Measures

If you're using a BigCommerce or Shopify ecommerce site, you don't have to build in a lot of protections. Humans really are the critical piece of your site security. They're the weakest link.

For that reason, access permissions and passwords should be your biggest point of focus. Of course, the level of security measures, training, and forced updates will depend on the reception and size of your team.

There are always tradeoffs to certain protective measures. If you were to lock everything down and make it exceedingly secure to the point where it inhibited jobs, slowed processes, and generally made everyone feel untrusted or even watched, you'd likely face a few resignations.

What it comes down to is balance.

Humans may be the weakest link in your security, but you need to find a reasonable mix for your company and the situations you face.

Our security experts tout these ecommerce security measures as your best actions to protect against the kinds of attacks plaguing ecommerce stores today.

Build a Security Culture in Your Company

"Culture" is one of those things we see touted in job postings, but security culture is a bit different in that it's a matter of enforcement, training, and enactment of the right tools and software.

It's more a matter of policy and adherence, but the cultural part of it surrounds the mindset and habits of each and every one of your employees.

90% of successful cyberattacks occur because of human error, as we've mentioned. In the office space (or in a home office), that may look like a simple email or even a Slack message saying something like, "Hey, I lost access to the VPN. Could you reset my password?" This is exactly the same scenario that caused the hijacking of 130 high-profile Twitter accounts, like that of Former President Obama.

So, what can you do to build a security culture?

Require Face to Face Verifications

Luckily, building a security culture doesn't have to be difficult. It's largely a matter of training and policy. Establish policies that make it clear to employees that security is everyone's responsibility.

For instance, each time an employee receives a request for a password, password change, or access to a restricted document or software, require all of your employees to connect face to face to confirm the request.

Usually, a Zoom call is enough (if you're not in the same office).

Creating this culture of security will help empower your employees to speak up if they see something strange or suspect they've encountered a phishy or otherwise malicious email. Let everyone in your organization know that security is a team sport, and they are expected to play ball.

Use Security Tools

Security tools like JAMF protect your store against ecommerce hackers by pushing out software updates, rotating passwords, and enforcing your password policies.

You simply install this program on everyone's computer and laptop if they use it for work.

Data Backups

Now, you might be thinking "I'm good—all my data is in the cloud!"

Sorry to say, but it doesn't matter.

The cloud still loses data (40% of SaaS application users already have), and it doesn't automatically back up things like your blog posts, inventory, orders, and product images. As Rewind CTO and co-founder James Ciesielski reminds us, "Just because something is saved 'in the cloud', doesn't mean it's secured".

Also, cloud platforms don't offer account-level backups.

SaaS platforms back up all of the data on their platform all at once, with no way to separate which data belongs to which user. The only way to restore individual account-level data is with an independent backup and recovery solution. Regularly backing up the data your business stores on cloud platforms protects your bottom line against downtime caused by data loss.

With a backup and recovery solution, like Rewind, covering your cloud data, it doesn't matter if you make a mistake, trust a buggy app, or fall victim to cybercrime - you can simply restore from your latest backup and get back to business.

(See all the measures we take to protect your backed up data)

How often should you backup data?

There are no set rules on this, but when it comes to backups, more is better. While a weekly backup is better than nothing, daily backups provide more extensive coverage. What if you update your theme on Monday, but only take backups on Sunday? If you suffered data loss on Friday, you'd have to start over again on the previous week's work. Daily or even continuous backups are the best choice to protect it all.

Reduce Your Attack Surface

So, an attack surface is essentially the plain of possible entry points or vulnerabilities that a hacker or botnet can exploit.

If you're using Shopify or BigCommerce, this attack surface is going to be significantly smaller because they're typically not sharing a server with anyone else, and they have a long history of security.

Your biggest vulnerability with the website itself lies in your web application updates. If you're late on updates, either of your firewall or your applications, bots may have figured out a way through those vulnerabilities. So the solution is to update your web applications and firewalls as soon as updates become available (but don't forget to check that the web application didn't change hands).

The other problem:

Now, it doesn't really matter how secure your hosting platform is, you can enact all the security measures in the world, and still face attacks from human error.

Say you have just 20 employees, and each of them use their private phones and laptops for work. That means your attack surface has at least 40 possible entry points (20 employees x 2 devices each).

Remember, Robin Hood and Twitter are both very large and secure companies, but both gave administrative access to support staff who weren't trained in their security policies. The administrative passwords became vulnerabilities that were used to take over multiple accounts.

The solution here is to reduce your attack surface by only allowing employees that absolutely need phone access (such as remote workers) to log into your company accounts and that they have the proper password training.

Main consequences of data breach:
lost data (60), compromised accounts or credentials (52), ransomware infections (47), malware infections (29)

Signs of a Cyber Attack on an Ecommerce Website

The first thing to know is that cyber-attacks aren't usually carried out by very complicated tools. They're simply automated systems looking for a vulnerability.

Tyler Kennedy, Application Security Engineer at Rewind, explains these botnets best:

"...A botnet is just a collection of compromised machines that can be used for attacks... [such as} using somebody's Smart TV, connected speakers, or other internet-connected devices to launch coordinated attacks.

But while most botnets simply exploit vulnerabilities, some malware is sophisticated enough to avoid all detection, even when you're poking around for signs of the attack script- such as the case Daniel mentioned earlier.

To spot those attacks:

You'll almost always have to hear something from the customer.

They've encountered some kind of glitch while using your site, haven't received products they've paid for but you can't find them in your system... there are plenty of issues that they'll likely spot long before you.

A responsive and alert customer success team is actually one of the best cybersecurity tools an ecommerce business can invest in. They'll often pick up on those queues from customers much faster.

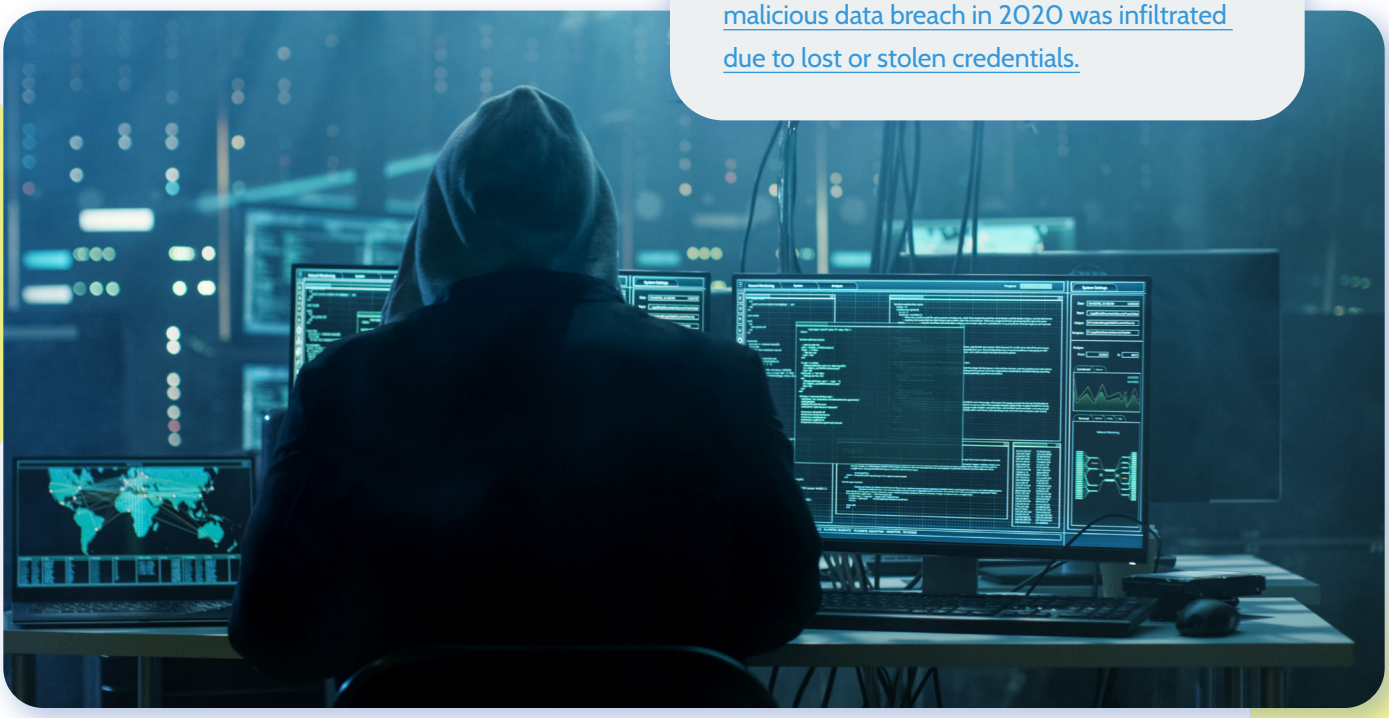
To verify it's a cyberattack:

It might take a little digging to judge whether or not it's a legitimate security issue and someone is exploiting credentials or stealing money from customers.

If you hear something from your customers, check the following:

- The URL the customer landed on—check to make sure they haven't fallen for a script-spoofing, phishing, or unicode attack
- Any screenshots your customers can provide
- Their account of what they saw on your site

Nearly one in five companies that suffered a malicious data breach in 2020 was infiltrated due to lost or stolen credentials.



Key Points on How to Secure an Ecommerce Website

By now you should have the understanding that most of the issues you face in securing your website come down to human error and access permissions, and that most attacks are automated.

To secure your ecommerce shop, you should:

- Use password managers across your company.
- Regularly check your web application ownership and permissions to make sure nothing's changed.
- Use antivirus tools such as a firewall to keep most of those automated attacks from scanning personal information from customers and your business.
- Establish a security culture by encouraging better, stronger passwords, locking screens when they're away from their computers, and using a VPN when not in the office.

Cybersecurity measures and methods of hacking (especially botnet capabilities) change quickly. Remember, they're running a business, so it's lucrative to them to get around all of your protective measurements. But if you're constantly changing/updating your own security and making it really costly for them to even attempt to penetrate, your store becomes a less desirable target.

So while it's impossible to make your store 100% impenetrable, it is possible to put in place the right security measures to make cyberattacks less of a possibility. But without the vital information powering your store, an ecommerce business is just a web domain, so you must protect your business-critical data too.

If you do, a cyberattack is much easier to come back from, with much smaller losses. Cloud backups of your ecommerce data ensure you can recover quickly in the event of a cyberattack (or any other data disaster, from rogue apps to spilled coffee).

FTC Received 2.2 Million Fraud Reports from Consumers in 2020.

Checklist

Measures to Secure Your Ecommerce Store

- [ ] Create a password policy and enforce good password health
- [ ] Add cybersecurity training to employee onboarding and ongoing training
- [ ] Install an update and security enforcer like JAMF
- [ ] Install a password manager on every computer and employee device used for work
- [ ] Install a firewall
- [ ] Update ecommerce web applications immediately upon release (automatic updates are a good idea here)
- [ ] Purchase a VPN for all remote workers to use
- [ ] Reduce your attack surface by restricting access and permissions to data and passwords
- [ ] Continually backup your business-critical data

Start your free trial of Rewind Backups for Shopify and Rewind Backups for BigCommerce today. Reach out to sales@rewind.com for a custom demo.

CONTACT US

rewind