Ecommerce security

A good ecommerce security strategy is vital to the success of any online business.

Threats can come from many different sources, and 88% of professional hackers can infiltrate an organization in just 12 hours, according to a Data Prot study.

With the risk of unauthorized access to your company's data looming around the corner, you need protect yourself from potential reputational damage and disruptions to your business.

While many ecommerce companies use some baseline security measures, staying vigilant is difficult when hackers constantly change their methods of attack. Merely hoping that you have the right solutions in place isn't good enough.

Understanding and implementing the methods your ecommerce company can use to secure your online store is key to safeguarding your data.

What is ecommerce security?

Ecommerce security is a set of guidelines that ensures safe online transactions.

Just like physical stores invest in security guards or cameras to prevent theft, online stores need to defend against cyberattacks.

According to the 2020 Trustwave Global Security Report, the retail industry was the most-targeted sector for cyberattacks.

In order to adequately protect your company from attack, you first need to know four key terms that are essential to understanding ecommerce security protocols.

Privacy

In the context of ecommerce security, privacy involves preventing unauthorized internal and external threats from accessing customer data.

Disrupting customer privacy is considered a breach of confidentiality and could have devastating consequences for your customers' privacy and your reputation as a retailer.

Privacy measures include antivirus software, firewalls, encryption, and other data protection measures.

Integrity
Integrity refers to how accurate a company's customer data is. Maintaining a clean, curated customer dataset is critical to running a successful ecommerce business.

Using incorrect customer's data — such as their phone number, address, or purchase history — causes people to lose confidence in your ability to protect their data and in your company as a whole.

Authentication
Authentication proves that your business does what it claims and that customers are who they say they are.

Your site should have at least some proof that it sells what it says it does and delivers those goods according to expectations.

Using customer quotes throughout your website and publishing case studies are two strategies for adding to your business's credibility.

Customers should also be required to verify their identities before processing their online transactions.

Requiring two-factor authentication or using magic links to log customers into their accounts are examples of customer authentication.

Non-repudiation
Non-repudiation means neither a company nor a customer can deny transactions they've participated in.

Non-repudiation is somewhat implicit in physical stores but pertains to online purchases as well.

Non-repudiation measures like digital signatures ensure that neither party can deny a purchase after it has been made.

Common ecommerce security threats

There are a multitude of different cyberattacks that could threaten your online business.

It's crucial to know what these threats are and how to prevent them.

The best way to get started is to make sure you understand the basic types of ecommerce security threats.

Phishing

Phishing is a method of cyberattack that tricks victims into providing confidential personal information — like passwords or social security numbers — via email, text, or phone.

Phishing messages convey urgency and come from addresses or phone numbers similar to those their targets interact with frequently.

Hackers will take other measures to make it seem like they represent a trusted company, like including links to pages that mimic sites the victim would recognize.

But phishing only works if customers provide the information attackers are requesting.

Informing customers that you will never email or text to ask for personal information will help them stay vigilant.

Malware and ransomware

Malware — short for "malicious software" — is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

For example, ransomware is a type of malware that encrypts a victim's files until they pay the attacker to release them.

Malware has the potential to cause major inconveniences for you, your employees, and your customers.

Attacks can slow your business to a halt and lock you out of critical systems. And removing malware is expensive.

Preventive measures like installing antivirus and antispyware software, keeping your systems updated, and using secure authentication can thwart these malware attacks.

SQL injection

While storing data in a structured query language (SQL) server database is a fairly normal practice, it's not automatically secure. SQL servers store data in a series of tables that can be retrieved by applications using requests or "queries."

If these servers are unprotected, attackers can write and inject their own queries, giving them access to view or change any information in an SQL database.

Providing security training to your developers, treating any edits to data tables as untrusted, and adopting modern web development technologies are good first steps to SQL injection (SQLi) prevention.

Cross-site scripting (XSS)

Cross-site scripting (XSS) occurs when an attacker inserts a piece of malicious code into a web page. Although XSS doesn't impact the entire site, it exposes customers on that page to cyberattacks like phishing and malware.

Scanning regularly for vulnerabilities in your website's code or API integrations and patching them quickly can help hinder XSS attacks.

Brute force attacks

Brute force attacks are an attempt to gain access to your site by targeting an online store's administrator console and trying to figure out its password by "brute force."

Once an attacker establishes a connection to your site, they'll run automated programs called scripts to guess every possible combination of letters, numbers, and characters that could make up your password.

You can protect your ecommerce site by choosing a complex, strong password for your admin panel and changing it regularly.

Ask your customers to do the same for any loyalty accounts they create.

E-skimming
E-skimming is a method of stealing credit card information and personal data from payment processors on ecommerce sites.

In this attack, hackers gain access to checkout pages and capture payment information as customers type it in real time.

E-skimming can result from XSS, phishing, or brute force attacks.

To help prevent e-skimming you need to regularly push patches to your web server, vet your ad server code, and keep third-party APIs updated.

If your site has already been impacted by e-skimming, see if your cyber insurance covers any losses and shut down your shopping cart page to investigate and eliminate the source.

Spam
Spam is an irrelevant message that prompts users to click on malicious links.

Spammers often use email to spread these links, but they may also leave infected links in comments on a blog, social media post, or contact forms.

Spam impacts a website's security and slows browsing speeds.

Deleting unwanted comments and enabling reCAPTCHA on forms can help thwart spam attacks.

ReCAPTCHAs require users to enter a slightly distorted series of numbers and letters, which spam bots can't read.

Deleting any spam comments that do get through and performing a root cause analysis to see where they came from cannot only keep your form response reports clean, they can also help you determine a solution.

Bots
Bots are designed to scrape websites for pricing and inventory.

Hackers then gain access to the site and use this information to hike prices or add the most popular inventory to their shopping carts.

When customers can't buy what they want or need, sales decline and stores may experience negative reviews or bad press.

Putting reCAPTCHA tools on your site, checking your API connections, and blocking old browser versions are good ways to combat bots.

You can also set up alerts for unusually high web traffic, failed gift card validations, and failed login attempts, as these can be signs of bots trying to gain access to your site.

Trojan horses
Trojan horses are a type of malware disguised as useful programs.

Because Trojan horses seem benign, team members or customers may download them onto their computers, at which point malware code is activated and attackers can steal personal information.

Robust antivirus software and firewalls offer some protection, but you also need to remind staff members and customers to be wary of email attachments and to avoid unapproved third-party downloads.

Best practices for ecommerce security
Hackers are always inventing new strategies for stealing data.

In addition to protecting against known threats, there are some general best practices for ecommerce security.

1. Use multilayer security
Multilayer security is the practice of adding secondary or tertiary layers of security controls throughout a technology system.

If one layer is compromised, attackers have to penetrate at least one other layer to get the information they are seeking.

Multiple security layers adds more obstacles attackers have to break through to infiltrate your site.

One important layer is a content delivery network (CDN).

The best CDNs use machine learning to block threats and infectious traffic.

Another layer could be multifactor authentication for employees logging in to company systems and for customers logging in to their loyalty accounts.

When they enter their information, they'll need to enter another code sent to them via text, email, or authenticator app.

2. Secure your website with SSL certificates
Secure sockets layer (SSL) certificates verify a website's identity and serve as an encrypted connection.

SSL certificates protect credit card details and other potentially sensitive transactions that occur on your ecommerce website and prevent hackers from using your site as part of a phishing attack.

3. Use firewalls
Firewall software and plugins allow trusted traffic but keep untrusted connections off of an ecommerce site. Regulating traffic flow makes detecting any anomalies easier and stops them before they enter your network.

This makes firewalls especially useful for protecting against cyber threats like XSS, spam, and malicious SQL injections.

4. Install antivirus and antimalware software
Attackers often use stolen credit card information to place orders, which puts your store at risk of enabling fraudulent activity.

Antivirus and antimalware software uses sophisticated algorithms to flag malicious transactions and provide fraud risk scores to determine whether transactions are legitimate.

Regularly scanning your site can greatly reduce malware attacks.

5. Train your staff
All employees should be aware of regulations that protect customer information.

Enforcing password updates, limiting access to sensitive information, and requiring employee cybersecurity and privacy training are all steps you can take to decrease your liability.

And remember to revoke access to all systems when employees leave, so they can’t sell data to cyberattackers or commit cybercrimes themselves.

6. Educate your clients
Some lapses in security happen as a result of customer behavior.

Customers have logins to many sites and sometimes reuse the same password over and over.

Requiring long, complex passwords and reminding customers about the risks of phishing attacks decreases the potential for cyberattacks.