BIGCOMMERCE

Ecommerce Website Security



A secure ecommerce site isn't a nice to have; it's a must-have.

Online stores handle large amounts of sensitive data — from payment processing to personal information — and are, unfortunately, an appealing target for hackers, including threats like trojan horses and other malicious software.

In fact, SecurityMetrics found that 92.4% of analysed ecommerce sites had malicious, suspicious, or concerning security issues.

Needless to say, security should be a top priority for any platform or online business. A breach can permanently damage a company's reputation and destroy customer trust. Customers expect businesses to bear the responsibility of safeguarding their data. As new ecommerce security threats continue to rise, cybercrime is more frequent and dangerous.

Discover how online brands can build a secure site capable of withstanding any threat.

What is ecommerce security?

Ecommerce security refers to the protections in place to keep online stores and their shoppers safe against cyber threats. This includes measures like data encryption, secure payment gateways, firewalls, anti-malware software, and access control. These security solutions help prevent unauthorised access to sensitive information, such as customer data and payment details.

By ensuring robust security, business owners can protect against data breaches, maintain customer trust, and comply with regulations like PCI-DSS. Strong ecommerce security is essential for both safeguarding the business and boosting consumer confidence.

Privacy.

Protecting customer data — like names, addresses, and payment details — is essential for any online business to succeed. To build trust, businesses need a clear privacy policy that explains how they handle and protect this data.

Regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) give customers control over their data, and complying with these laws is key to maintaining customer trust and avoiding legal issues.

Integrity.

Integrity means maintaining transparency and trust in how businesses handle sensitive customer information. It involves being upfront about security measures, clearly communicating data protection practises, and ensuring they manage customer data responsibly.

When businesses operate with integrity, they take accountability for protecting customer information and swiftly address any security concerns or breaches. This fosters trust, as customers feel confident that their personal information and payment details are safe.

Authentication.

Authentication is critical to ecommerce security, ensuring that only authorised users can access sensitive information or perform specific actions on an ecommerce website. It involves verifying the identity of users through methods such as usernames and passwords, two-factor authentication (2FA), or biometric verification.

Strong authentication protocols help prevent unauthorised access to customer data, financial information, and business systems. Two-factor authentication (2FA), for example, adds an extra

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

layer of protection by requiring users to verify their identity through a second method, such as a code sent to their phone.

By implementing robust authentication measures, ecommerce businesses can reduce the risk of data breaches and build trust with customers, assuring them that their information is secure.

Non-repudiation.

Non-repudiation ensures that parties involved in a transaction cannot deny their participation or the authenticity of the transaction. This is key for businesses and customers, proving that actions like orders and payments are valid and legally binding.

Businesses can achieve non-repudiation through methods like digital signatures and encryption, which verify the identity of the participants and confirm that the transaction occurred. By using these measures, ecommerce platforms protect against fraud and provide a clear record for resolving disputes.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

Common cyber security threats facing ecommerce websites

Ecommerce websites are prime targets for cyberattacks due to the sensitive customer data and payment information they handle. Understanding these common threats is the first step in protecting an online store.

Phishing attacks.

Phishing is a common social engineering attack where hackers try to trick individuals into providing them with sensitive data. These scammers often do this through fraudulent emails, texts, or websites that ask users to input information like social security numbers, passwords, or payment details.

- **Impact on ecommerce:** Phishing attacks can seriously harm a business, resulting in financial damage and lost customer trust.
- **How to protect against it:** Phishing can target anyone, from employees to customers, making it essential to educate potential victims on how to spot phishing messages. Implementing email filtering and multi-factor authentication (MFA) can significantly reduce the success of phishing attempts.

Malware and ransomware attacks.

Malware and ransomware go back to the dial up modem days of the internet. Malware can damage systems and even disable computers. Meanwhile, ransomware is a type of malware that can lock out individuals unless they pay a ransom, with no guarantee they'll gain access back.

- **Impact on ecommerce:** Malware can steal sensitive company data, while ransomware can hold a site hostage, threatening the loss of vital information.
- **How to protect against it:** Implement and regularly update antivirus softwares and firewalls. In addition, properly educate employees on the risk of malware and ransomware attacks, which can occur through phishing or downloading suspicious material.

SQL injection.

An SQL injection is when a malicious query is submitted into a database. This provides hackers access to sensitive information, allowing them to view or modify it, and even publicly expose it. Platforms like WordPress, which often use SQL databases, need to ensure their security solutions are robust.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

- **Impact on ecommerce:** An SQL injection can lead to data breaches that leak private data such as names, addresses, and payment information.
- **How to protect against it:** Safeguard against SQL injection by validating user inputs, using parameterised queries, and deploying database security tools to detect and block potential attacks.

Cross-site scripting (XSS).

Cross-Site Scripting (XSS) involves inserting malicious code into a website, usually through JavaScript. This attack can impact the user experience by directing viewers to malicious sites and stealing user session data.

- **Impact on ecommerce:** XSS attacks ruin a website's reputation by stealing sensitive information, impersonating users, or taking them to a malicious site. In addition to damaging a brand's reputation, this attack can lead to data breaches and damage customer relationships.
- **How to protect against it:** Implement security measures like Content Security Policy (CSP) headers, practise secure codes, and validate user information.

E-skimming (magecart attacks).

In e-skimming, hackers steal sensitive payment information, such as credit card numbers, from online shoppers. Attackers typically inject malicious code into ecommerce websites or point-of-sale (POS) systems to steal credit card details as customers make purchases.

- **Impact on ecommerce:** E-skimming attacks involve stealing payment information from shoppers, leading to fraudulent transactions. This can result in a damaged reputation and cause customers to lose trust in a brand.
- **How to protect against it:** Practise secure coding and regularly cheque for malicious code. In addition, be sure to have secure firewalls and real-time monitoring solutions in place.

Distributed denial of service (DDoS) attacks.

A Distributed Denial of Service (DDoS) overloads a website with traffic from multiple sources, making it unavailable to users. In a DDoS attack, attackers use a large number of compromised devices to flood a website with traffic.

- **Impact on ecommerce:** Long periods of downtime due to DDoS attacks can result in lost revenue, frustrated customers, and lasting harm to a business's reputation.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

- **How to protect against it:** Implement protection services like Cloudflare, use traffic filtering, and scale server resources to manage traffic surges effectively.

Brute force tactics.

In a brute force attack, an attacker attempts to guess a user's login password by systematically trying every possible combination until they find the correct one. This method takes time and requires a lot of computing power, but it can succeed with weak or simple passwords.

- **Impact on ecommerce:** Brute force attacks can result in hackers gaining access to protected areas of an ecommerce website. This can result in data breaches, financial losses, and loss of control over the site.
- **How to protect against it:** Implement security protocols like two-factor authentication, a CAPTCHA verification, or rate limiting.

Account takeover (ATO) attacks.

An Account Takeover (ATO) occurs when hackers gain total access to a customer or employee account, whether through an attack like a phishing scam.

- **Impact on ecommerce:** An ATO account gives cybercriminals access to all data a specific user has access to. With this information, they can cause data breaches, make fraudulent transactions, or even lock out the real account holder.
- **How to protect against it:** Implement secure login policies, like MFA, password requirements, and limited login attempts.

Card-not-present (CNP) fraud.

A Card-Not-Present (CNP) fraud is when a cybercriminal buys products online with stolen payment information.

- **Impact on ecommerce:** This type of fraud can lead to financial losses and even damage a business's reputation, resulting in a loss of customer trust.
- **How to protect against it:** Put measures into place that help verify the true cardholder, like address verification and 3D secure authentication.

Man-in-the-middle (MITM) attacks.

A Man-in-the-Middle attack is when a cybercriminal non-threateningly positions themselves near a shopper while they're inputting their payment information. This allows them to steal sensitive

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

data, like login information or payment details.

- **Impact on ecommerce:** MITM attacks lead to data breaches and fraudulent transactions, causing shoppers to question their safety on a site.
- **How to protect against it:** Encourage shoppers to avoid making online purchases in public places, especially when using an unsecure Wi-Fi account. In addition, enforce HTTPS encryptions throughout the entire site.

Bot attacks.

Bots can attack in a variety of ways, like scraping content and performing credential stuffing. This is often with the intention to gain access to customer or employee accounts.

- **Impact on ecommerce:** Bot attacks can lead to data breaches and even disrupt business operations by altering stock information. This can result in a negative UX, leading shoppers to lose trust in a brand.
- **How to protect against it:** Protect against bot attacks by implementing CAPTCHAs and rate limiting.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

Managing internal ecommerce security threats

Not all security threats come from the outside. There are plenty of internal threats — some of them wholly unintentional — that ecommerce companies should be aware of.

Employee Negligence.

Many cyber-attacks are a result of employees failing to follow proper security protocols. While often unintentional, this can lead to the distribution of sensitive information, falling for phishing scams, or mishandling data.

- **Example:** An employee might accidentally click on a phishing email, prompting them to open a malicious link. This could result in dangerous malware downloading onto the company network, enabling hackers to access sensitive information.
- **How to mitigate:** Conduct regular security training that inform employees about the dangers of cyber attacks, what typical scams look like, and how to reduce the likelihood of being a victim of an attack.

Employee sabotage.

On the other end of the spectrum from negligence is intentional sabotage. While there's no surefire way of avoiding disgruntled employees, limiting access to sensitive data, enforcing strong password standards, and having regular access reviews will help mitigate damage.

- **Example:** A disgruntled employee with site editing permissions might try to adjust product information and pricing to negatively impact the business.
- **How to mitigate:** Closely monitor site access and check for unusual activity in sensitive system areas. Additionally, make sure all users are deactivated immediately upon termination.

Third-party insiders.

This expands employee sabotage to additional parties working with a company. Contractors, vendors, or even customers may be exposed to attackers, who then bring that contagion into a company's systems.

- **Example:** An agency partner with access to sensitive information could be the victim of a phishing scam, leaking customer data.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

- **How to mitigate:** Ensure partners are carefully vetted and follow strict security guidelines to help avoid a security incident.

Poor password hygiene.

Strong passwords are essential to keep hackers from accessing user accounts. Passwords that are weak or reused can easily be exploited by attackers, creating security risks that put an entire business in jeopardy.

- **Example:** An employee uses the same password for their work email and personal email account. If their personal account is compromised, an attacker can easily gain access to their work login credentials, putting their company at risk.
- **How to mitigate:** Use MFA and require strong passwords with character, symbol, and capitalisation requirements.

Misconfigured systems or software.

Another common internal threat is security misconfigurations. This could be granting too many users access to sensitive information or leaving data unprotected. These errors usually occur when a system is set up, deployed, or during routine maintenance.

- **Example:** An IT admin grants all employees access to highly sensitive company information without properly training them on security protocols specific to this data.
- **How to mitigate:** Ensure permissions are given only to employees who need them to complete their job duties. Regularly audit systems to ensure only employees in need of access can authorise sensitive information.

Unmonitored data access.

Data that is left unmonitored can open the door for cybersecurity threats. This means employees and external partners can access sensitive data for any reason without any oversight.

- **Example:** An employee accesses customer payment information to make fraudulent purchases, with no monitoring in place to detect the suspicious activity.
- **How to mitigate:** Review access logs and limit permissions based on job description and training completed. Implement monitoring tools to detect suspicious activity.

Lack of security awareness and training.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

When employees are not trained to recognise security risks, they can often fall into the trap of phishing scams and other cyber attacks. This can lead to the mishandling of sensitive data, which can be detrimental to a company.

- **Example:** An employee clicks a link to a suspicious email that downloads malware to the company software.
- **How to mitigate:** Ensure employees take regular in-depth training that teaches them the risks of cyber attacks and how to avoid them.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

Ecommerce website security best practises

Online businesses never want to be in the headlines for a security reason. Following these best practises will at least greatly reduce the chances of possible security issues.

Create a password policy for your company.

Require complex passwords that have at least eight characters, with a mix of upper and lowercase letters, numbers, and symbols. This should be mandatory for employees and customers alike.

Limit access to sensitive data.

Sensitive data should only be accessible by users and systems that absolutely need it. The fewer access points, the better.

Create a security plan for adding plugins and third-party integrations.

Brands should assess the third-party systems included in their tech stack and ensure they are fully up-to-date. They should evaluate the security of each system and confirm that it meets their own security standards.

Ensure compliance with PCI-DSS regulations.

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards that must be followed by any organisation that accepts credit or debit card payments. PCI compliance is mandatory, so businesses should stay up-to-date on any changes.

Choose a secure ecommerce platform.

Choosing a secure ecommerce platform is essential for businesses to protect their online stores. The platform should provide features like PCI compliance, SSL certificates, multi-factor authentication (MFA), and automatic security updates to safeguard customer data and ensure a secure shopping experience.

Use an SSL certificate.

Secure Sockets Layer (SSL) certificates are increasingly common in ecommerce and establish a secure, encrypted connection between a web server and browser.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

The SSL certificate verifies the identity of the website, and the encryption technology ensures that any data transmitted between the server and the browser remains private and cannot be intercepted or tampered with.

Two-factor authentication.

Today, most people are familiar with getting a code texted to them to log into a system. 2FA is much more common now and serves as a strong layer of defence and provides an additional step in confirming identities.

Keep your software up-to-date.

The software in a tech stack will likely receive regular updates and patches, which will include additional security. Brands should ensure all software is updated when necessary.

Train your employees and contractors on best practises.

Social engineering happens all the time and it's on the company to train and inform their workforce of how to avoid attacks. Companies should regularly test their employees with fake emails to see how receptive they are to phishing attacks.

Develop an incident response plan.

While businesses strive to prevent attacks, owners must always be prepared for the worst. It's crucial to have a comprehensive response plan in place for potential breaches, covering identification, mitigation, and communication.

Regular security audits and vulnerability scanning.

Regular security audits and vulnerability scans help identify weaknesses in ecommerce systems, such as outdated software or security flaws. Conducting these checks proactively allows businesses to address issues before they become serious threats and ensures ongoing data protection.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

Ecommerce website security compliance considerations

There are standards — both legal and industry — that every ecommerce company needs to meet. This does not guarantee a secure platform, but meeting these does help protect customer information.

Payment Card Industry Data Security Standard (PCI-DSS).

Any entity that processes credit card transactions must meet PCI-DSS standards. These guidelines protect credit card information, from storage to checkout.

General Data Protection Regulation (GDPR).

The European Union enacted GDPR to protect the personal information of all EU citizens. This applies to businesses that exist outside the EU but sell to Europeans as well.

California Consumer Privacy Act (CCPA).

The CCPA is similar to the GDPR, but is specific to the state of California only. It's the strictest standard currently in the United States.

Australian Privacy Act (APA).

The APA regulates how Australian businesses handle personal data. This act impacts all businesses that collect data from Australian citizens.

ISO/IEC 27001 (Information Security Management).

ISO/IEC 27001 is a global security standard designed to protect data through risk management. Ecommerce brands can obtain an ISO/IEC 27001 certification by integrating an information security management system (ISMS), performing routine security audits, and following data safety best practises.

ISO/IEC 27701 (Privacy Information Management).

In addition to information security management, ISO/IEC 27001 also encompasses privacy information management — meaning it provides a framework for protecting personal data. Businesses can comply with this policy by ensuring privacy standards are followed across their entire business, conducting privacy audits, and implementing privacy controls.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

ISO 22301 (Business Continuity Management).

ISO 22301 is a global standard that allows for businesses to resume normal operations following an event like a cyber attack. This policy is essential to keep businesses functioning in the wake of a disruption. In order to comply with this policy, businesses should develop and regularly test their business continuity management system (BCMS), and devise an action plan with clear roles if an event like this occurs.

SOC 1, SOC 2, and SOC 3 Compliance.

SOC assesses how businesses manage customer data regarding financial reporting (SOC 1) and security and privacy (SOC 2). SOC 3 provides a public record of this assessment. Cloud-based brands should strive to follow SOC compliance and implement proper protocols to ensure the safety of customer data.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

How BigCommerce approaches ecommerce security

BigCommerce prioritises ecommerce security by implementing advanced security measures that protect both businesses and their customers. Through proactive tools like encryption, secure payment gateways, and regular security updates, BigCommerce ensures a safe and trusted online shopping experience. Visit our platform trust centre to learn more about how we protect yours and your customers' data.

Trusted cloud infrastructure.

BigCommerce uses the Google Cloud Platform to provide brands with the most flexible and secure hosting infrastructure. This multi-layered security approach includes 24/7 monitoring, perimeter firewalls, and strict adherence to PCI DSS standards, ensuring the highest level of protection for customers. By leveraging Google Cloud, BigCommerce provides businesses with a scalable, resilient platform that mitigates threats like DDoS attacks, while freeing them from the burden of server maintenance and security updates.

PCI DSS level 1 compliance.

BigCommerce is certified as a PCI DSS 3.2 Level 1 Service Provider, the highest level of compliance in the payments industry. This certification ensures robust protection against credit card data breaches, covering areas like access management, infrastructure security, and incident response. By meeting these strict standards, BigCommerce eliminates the need for customers to manage complex compliance requirements themselves, saving both time and resources.

Encryption and data security.

To enhance site security, boost shopper trust, and improve search rankings, BigCommerce ensures robust encryption and data security by enabling HTTPS for all stores. The platform supports the latest versions of TLS (v1.2 and v1.3) for the strongest encryption, while automatically provisioning free SSL certificates for custom domains. Customers can also opt for third-party TLS certificates or extended verification with True BusinessID for added security.

Multi-Factor Authentication (MFA).

By default, BigCommerce staff user accounts are protected with email verification in addition to the standard username and password. For enhanced security, customers can enable 2FA, which adds an extra layer of protection by ensuring only authorised users can log in and manage the store.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

ISO Compliance.

BigCommerce is PCI DSS 4.1 Level 1 Attestation of Compliance, ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO 22301:2019, ISO/IEC 27017:2015, ISO/IEC 27018:2019, meaning it follows a comprehensive and continually improving approach to security management. This certification sets the standard for managing information risks through an ISMS and best practises. With PCI DSS 4.1 Level 1 Attestation of Compliance, ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO 22301:2019, ISO/IEC 27017:2015, ISO/IEC 27018:2019, BigCommerce ensures top-level security and protection for sensitive data across its platform.

Data backup and disaster recovery.

All BigCommerce store data is replicated across four geographically separated data centres, ensuring redundancy and high availability. Production servers are backed up daily to remote servers, protecting customer data, even in the event of a disaster that affects all production data centres. This backup process guarantees that customer data can be restored on alternative servers, minimising downtime and ensuring business continuity.

Regular security audits and testing.

Regular security audits and testing are critical to ensuring a secure ecommerce environment. BigCommerce conducts ongoing audits, vulnerability scans, and penetration testing to identify and address potential security risks, protecting both businesses and their customers.

Access control and monitoring.

BigCommerce boosts security with Role-Based Access Control (RBAC), ensuring users can only access the areas they need, keeping sensitive data safe. The platform also monitors activity logs to spot and respond to any unusual or unauthorised actions.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

The final word

Security is critical not only for keeping ecommerce businesses running smoothly but also for maintaining customer trust. When customers share their personal information, they rely on ecommerce companies to protect their data.

From using Web Application Firewalls (WAF) and Content Delivery Networks (CDN) to safeguarding credit card information, it's the responsibility of online stores to implement strong security measures that ensure data is protected at every step.

Discover how countless brands have securely scaled with the help of BigCommerce.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE

FAQs about ecommerce website security

Why is ecommerce website security a top priority?

Ecommerce sites receive and store a large amount of online transactions and user data — data that is of particular interest to hackers. Cyber threats are a constant, neverending battle and are always evolving as new and more sophisticated ways to attack are developed. It's on the business to keep the site — and customers — safe and secure. Good security practises lead to good security protocols.

What are examples of ecommerce data breaches?

Data breaches don't just hit small businesses with limited resources. Even some of the world's biggest brands have been victims of cybercriminals. adidas: The global shoe company has been hit hard in the past. In 2018, the company's US website had customer contact information exposed. Mercari: Mercari is a Japanese ecommerce company that operates an online marketplace. In 2021, the company disclosed a major data breach incident. Target: Target's ecommerce store was affected by one of the largest data breaches in history. In 2013, millions of customers were impacted by a cyber attack that exploited vulnerabilities in the company's payment gateway, allowing hackers to steal payment card information such as credit and debit card numbers, expiration dates, and CVV codes.

What is personal data?

Personal data is any information that can identify someone. This includes a person's name, address, phone number, email address, social security number, passport number, date of birth, and any other information that can be linked directly or indirectly to their identity.

What is Multi-Factor Authentication?

Multi-factor authentication is a security functionality that requires multiple forms of authentication to verify a user's identity. This provides an additional layer of security against cybercriminals.

What is the International Organisation for Standardisation (ISO)?

The International Organisation for Standardisation (ISO) is an independent, non-governmental organisation that develops and publishes standards for various industries and sectors. In May 2023, BigCommerce earned ISO 22701 and ISO 22301 certifications.

Growing your high-volume or established business?
Start your 15-day free trial, schedule a demo or give us a call at +61 2 8188 1832.

BIGCOMMERCE