

Safe & Secure



5 Essential Security Headings for Your eStore

1. Why Your Password Matters:

Your password is like the key to your online accounts, so it's crucial to make it strong and unique. Avoid using easily guessable passwords like "password123" or common words. Instead, create a password that combines uppercase and lowercase letters, numbers, and special characters. Consider using a passphrase, which is a series of words or a sentence that's easy for you to remember but hard for others to guess.

2. Spotting Online Scams:

Watch out for scams like phishing emails and fraudulent websites. Be cautious with unsolicited emails asking for personal or financial info. Verify sender's email, watch for errors, and contact the company directly if unsure.



Opayo, previously known as Sage Pay

Sage Pay (Opayo)

Opayo Payment Gateway has implemented an update effective March 31st 2024, removing all previous API URLs. We've already made these adjustments to our live websites, ensuring everything is secure. Extensive testing over weeks confirms the smooth functionality of these changes.

3. Keeping Your PC Secure:

The primary reason for keeping your PC and programs up to date is security. By promptly applying updates, you protect yourself against a wide range of cyber threats, including malware, ransomware, and phishing attacks. These updates not only fix known vulnerabilities but also strengthen your computer's defences against emerging threats.

4. End-to-End Encryption:

End-to-end encryption makes sure your data stays private and secure while it travels from one place to another. Only the sender and receiver can read it. This is crucial for keeping sensitive info safe, like personal messages, money transactions, and medical records from unauthorised access.

5. Biometric Authentication Passwords:

Biometric authentication uses fingerprints or facial features to verify identity, offering stronger security than passwords. It's convenient, eliminating the need to remember passwords; you simply use your fingerprint or face to unlock your device or log in.

Quick Tip: Clicked on a Phishing Website?

- **Close the Website Immediately:** Don't interact with any links or buttons.
- **Disconnect from the Internet:** Prevent further communication with attackers' servers.
- **Scan Your Device for Malware:** Use antivirus software to remove any threats.
- **Change Your Passwords:** Secure affected accounts with strong, unique passwords.
- **Monitor Your Accounts:** Watch for unusual activity.