

## Website Security Features

Know your data is safe and secure from unauthorised access.

Here are some essential features Safe2Open.net encapsulates:



**1. End-to-End Encryption:** All data transmitted between the user's device and the server should be encrypted using robust encryption protocols like TLS (Transport Layer Security) or SSL (Secure Sockets Layer). Hypertext Transfer Protocol Secure (https) is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol. TLS is an authentication and security protocol widely implemented in browsers and Web servers. SSL works by using a public key to encrypt data transferred over the SSL connection. Most Web browsers support SSL. It allows you to communicate securely with the web server.

**2. Two-Factor Authentication (2FA):** Implementing 2FA adds an extra layer of security by requiring users to provide several forms of verification before accessing their accounts, such as a password along with a code sent to their email.

**3. Regular Security Audits and Penetration Testing:** The website will undergo frequent security audits and penetration testing conducted by reputable third-party security firms to identify and address vulnerabilities before they can be exploited by malicious actors. See [Go Daddy Data Protection Standards](#)

**4. Data Encryption at Rest:** All stored data is encrypted to protect it from unauthorised access, even if someone gains physical access to the server or storage devices.

**5. Strong Password Policies:** Enforcing strong password requirements, such as a minimum length, complexity, and expiration period, can help prevent unauthorised access due to weak passwords.

**6. Secure Coding Practices:** Developers have adhered to secure coding practices to minimize the risk of common vulnerabilities such as SQL injection, cross-site scripting (XSS), and buffer overflows.

**7. Strict Access Controls:** Implementing role-based access controls ensures that users only have access to the data and functionalities necessary for their roles within the organisation. For example, all admin users of Safe2Open cannot see safe combinations or key locations. These are restricted to the User and the Police only.

**8. Regular Software Updates and Patch Management:** Keeping all software components up to date with the latest security patches helps prevent exploitation of known vulnerabilities.

**9. Logging and Monitoring:** Comprehensive logging of user activities and system events, coupled with real-time monitoring, allows for the detection of suspicious behaviour and timely response to security incidents.

**10. Compliance with Data Protection Regulations:** Adhering to relevant data protection regulations such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act) ensures that user data is handled in a lawful and ethical manner.

**11. Secure File Transfer:** As our website involves file transfer, we have implemented secure file transfer protocols like SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure) ensures the confidentiality and integrity of transferred data.

**12. User Education and Awareness:** Providing resources and guidelines to educate users about best security practices, such as avoiding phishing attempts and safeguarding their accounts, will help mitigate risks associated with human error. Repeating email and password sign-in allows for fewer mistakes.

**13. Incident Response Plan:** Go Daddy have a well-defined incident response plan in place ensures that the organization can efficiently respond to security incidents, minimise their impact, and restore normal operations as quickly as possible.

**14. Data Backup and Disaster Recovery:** Regularly backing up data and implementing robust disaster recovery plans help mitigate the risk of data loss due to unexpected events such as hardware failures, natural disasters, or cyberattacks. See [Go Daddy Back up](#)

**15. Transparent Privacy Policies:** Clearly communicating the website's privacy policies, including how user data is collected, stored, and used, fosters transparency and trust with users. See policy section at the bottom of the webpage

Safe 2 Open\* Leadership Team

11<sup>th</sup> March 2024

\* Safe 2 open is a trading name of TWH holdings Limited