Scholarly Space Security

At Scholarly Space, the security of your data is our highest priority. We've implemented multiple levels of security to protect and back up your data.

Types of Data Stored:

We store two distinct types of data: '*User Data*' and '*User-Generated Content.*'

User Data is data regarding a user's identity and consists of:

- **ID:** An ID is a unique 21-digit integer assigned to each user. If a user signs-in with Google, Google provides this private ID. This ID is inaccessible to everybody, even to the user who is associated with the ID. If a user signs-up through Scholarly.Space, a unique 21 digit integer is randomly generated and assigned to the user in question.
- **Email:** We store the email address that a user signs-in with. This is

either the email address associated with their Google Account, which we access via Google OAuth, or it is the email address the user signed-up with through Scholarly.Space.
- **First Name**
- **Last Name**
- **Image URL (if applicable):** If a user signs in via Google OAuth, we store the URL address of their user image: their public 'profile' image associated with their google account.

User-Generated Content is data the user uploads through our website. User-Generated content is tagged with the user's unique 21 digit ID and consists of:

- **Posts:** A post refers to a document a user submits and uploads through our proprietary posting and commenting system. Each post is stored as an individual document in the MarkDown format (.md).
- **Comments:** A comment refers to a document a user submits and uploads through our proprietary posting and commenting system. Each comment is stored as an individual document in the MarkDown format (.md).
- **Module Information:** Module Information is the information generated or provided when creating a new 'module,' and consists of the module title, module type (project, club, independent study, etc), module url (either external or internal), module sector (mathematics, science, literature, etc), module career cluster, (health science, education & training, hospitality & tourism, etc), and the module id (a unique, randomly-generated 5 digit integer referencing the module).

How Data is Stored:

User Data:
User Data is stored in a password-protected and AES-256 encrypted MySQL database. MySQL is widely used and meets the highest standards of data security. Click here for more information on MySQL.

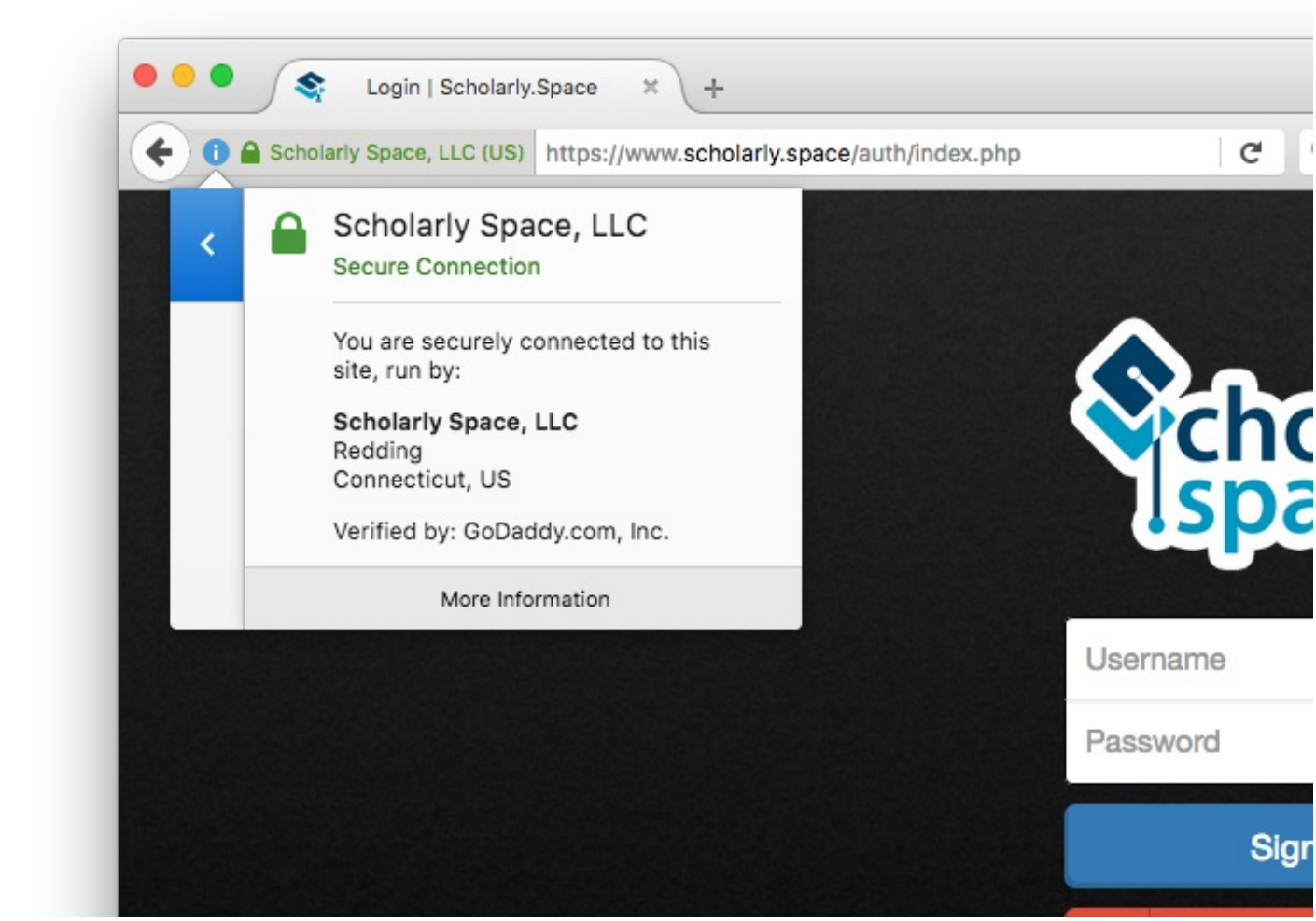
User-Generated Content:
Scholarly Space's servers are programmed to require a password in order to access student-generated content. Our proprietary posting and commenting system stores data in such a way that it is inaccessible to the public. When a student logs-in and requests to view or make either a post or a comment, our server validates the user to ensure they have the correct permissions. If a user passes validation, the server will use a secure *Content-Access-Password* password to 'unlock' read/write permissions solely for the information requested. This password is stored on a private part of the server, making it virtually impossible for a malicious user to gain access to. We also disable directory access on our servers, meaning that users are unable to see the data structure of our website. Furthermore, all of the code used to interact with database content is written in PHP. PHP is executed on the server, not on the user's computer (unlike JavaScript, CSS, HTML, etc.) The PHP code is never visible to users which means that users are unable to gain information on how our server's communicate with secure data.

In Transit

Scholarly Space uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to protect data in transit between Dropbox apps and our servers; This is designed to create a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption.

When a browser attempts to access a website that is secured by SSL, the browser and the web server establish an SSL connection using a process called an "SSL Handshake." Note that the SSL Handshake is invisible to the user and happens instantaneously. Essentially, three keys are used to set up the SSL connection: the public, private, and session keys. Anything encrypted with the public key can only be decrypted with the private key, and vice versa. Because encrypting and decrypting with private and public key takes a lot of processing power, they are only used during the SSL Handshake to create a symmetric session key. After the secure connection is made, the session key is used to encrypt all transmitted data.

Scholarly Space is proud to use SSL EV, the most highly-trusted way to secure an SSL connection. An Extended Validation Certificate (EV) is a public key certificate that proves the legal entity controlling a web site or software package. Obtaining an EV certificate requires verification of the requesting entity's identity by a certificate authority. EV certificates are used when establishing HTTPS connections between web browsers and web servers. See certificate below:



Security Practices

Scholarly Space also implements a multitude of security practices to ensure our high-level of security is upheld.

Scans, Backups, and Intruder Detection

Scholarly Space performs daily malware scans across its entire server. If a security threat is found, it is removed from the server automatically. In addition to this, we monitor all the file changes that occur across the server in order to detect unauthorized access to the site. Scholarly Space also has implemented DDoS protection, SQL Injection prevention, and XSS Injection prevention.

We are continuously performing data backups to ensure that our users' data remains safe and secure.

We will notify our users (and their parents where applicable) as soon as practical, but not later than 48 hours after we become aware of, or suspect, that any user record under our control has been subject to unauthorized access or suspected unauthorized access.

Regular Password Changing

Scholarly Space uses several server-side passwords to secure our database tables and content. These passwords are randomly generated and consist of numbers, lowercase letters, uppercase letters, and symbols. We change all of our passwords weekly.