Cyber Security Information

While File13F.com does not receive, send or maintain non-public information, we have designed a back-end structure able to pass all cyber security benchmarks. To do so, File13F.com has partnered with SendSafely to transport encrypted data and DigitalOcean to process data in our software.

SendSafely Cyber Structure and Policies

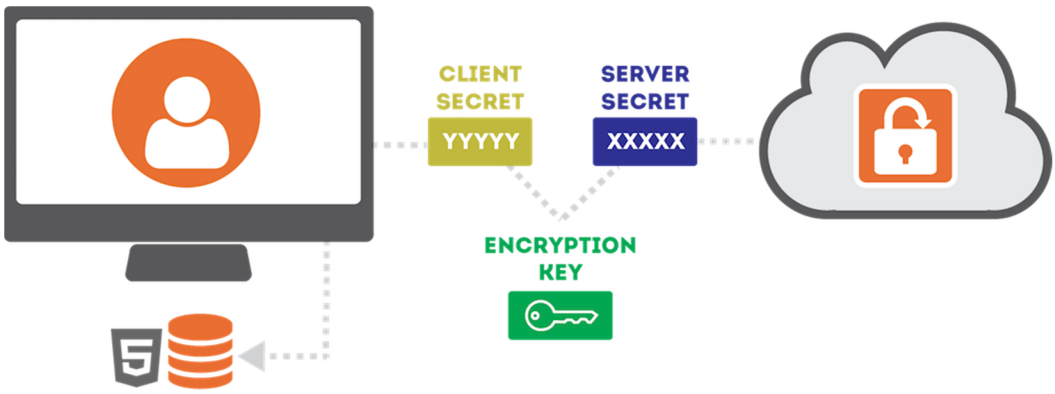
Security Overview

SendSafely uses several layers of security to protect your information.

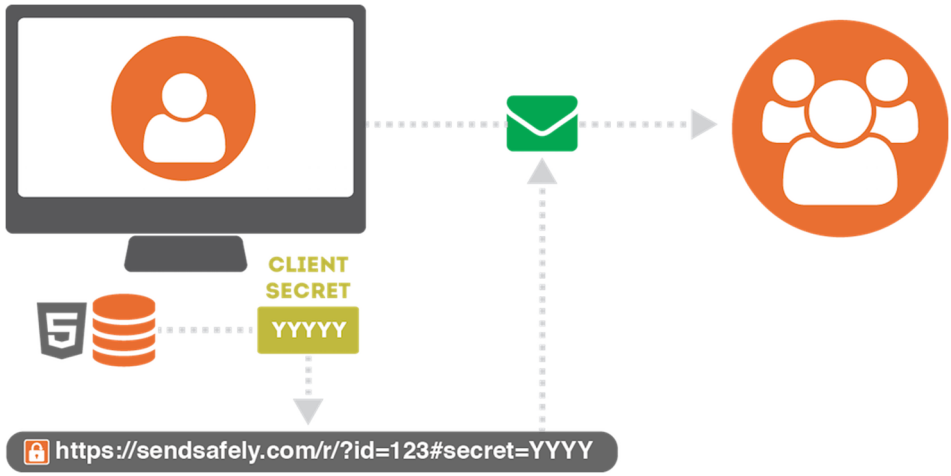
All files and messages you send through our platform are protected using end-to-end encryption. End-to-end encryption means that nobody other than you and the individuals you authorize can read them. There is no way for SendSafely, or any third party, to decrypt this information. Even if the data is intercepted, stolen or seized, it cannot be read without the proper decryption keys, which are never stored or accessible by our systems.

Every set of files or messages that you send through SendSafely are encrypted on your machine before being submitted to our servers. We use the OpenPGP message format, with a key that is derived using OpenPGP's Iterated and Salted (Type 3) String-to-key (S2K) specifier. The Type 3 S2K converts a variable length pass-phrase into a 256-bit symmetric AES encryption key. The pass phrase that is used consists of 512 random bits of data and is a combination of the following two values:

- A 256-bit random secret value that gets generated by our servers (referred to from here on as the **Server Secret**)
- A 256-bit random secret value that gets generated by your machine (referred to from here on as the **Client Secret**)



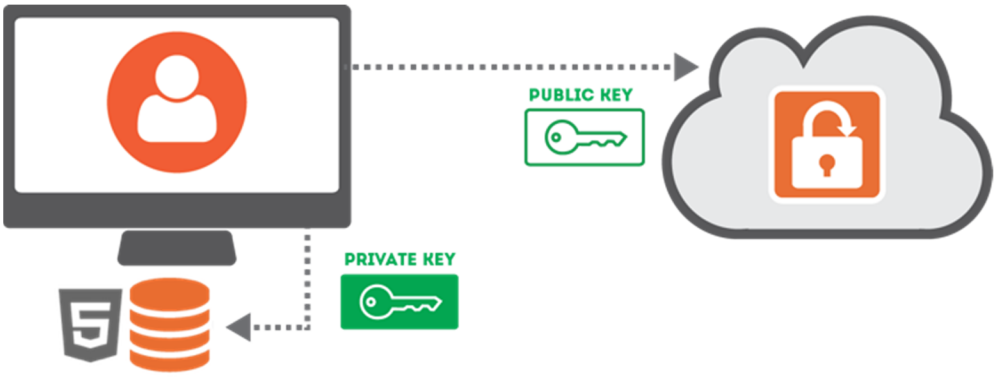
The Server Secret is stored by us, and provided to your recipients along with the file once we verify their identity. The Client Secret, however, is never disclosed to our servers and remains on your machine at all times. The Client Secret is sent directly by you to them within the Secure Link needed to access the items. When you want to share access with someone else, you (the sender) provide them each with a Secure Link that includes the Client Secret embedded within URL Fragment Identifier.



Because this value is embedded within the URL Fragment Identifier, it is never visible to our server (even when the link is clicked by the user). Instead, the value is used by our client-side API and combined with the Server Secret to recomputed the AES Key needed to decrypt the items.

Trusted Device Keys

Trusted device keys are a secondary encryption method we use to make it easy for you to access items. Any time you log in from a new browser, SendSafely will ask you if you want to trust the browser. If you choose YES, your browser generates a 2048-bit RSA Public/Private key pair. The private key is never submitted to SendSafely, it gets stored in your browser's local storage. The public key gets uploaded and stored by SendSafely.



Once you have a trusted browser, the server will provide a copy your trusted browser public key to users that send you items. The public key is then used to encrypt a copy of the Client Secret for that item, and the encrypted Client Secret gets uploaded to SendSafely. This lets us provide you with access to all of your received items using a trusted browser, eliminating the need for the sender to share a secure link with you.

Local Storage Encryption

SendSafely's security model relies on storing private key material within your browser's HTML5 Local Storage. Your browser automatically protects this information by making sure that other websites are not allowed to access the information we store there. As an additional safeguard, SendSafely encrypts this information using a 128-bit AES key that is unique to your user account. The key is generated by us when you create your account, and stored on our servers. We only reveal this key to your browser while you are logged into our site. That way if someone else gains access to your local storage, the SendSafely information we store there cannot be viewed.

Two Step Login

Users have the option of enabling Two Step Login on all SendSafely accounts. When Two Step Login is enabled, we generate random 6 digit PIN ever time you log in from an unrecognized device and send it to your mobile phone. The PIN is required, in addition to your user-id and password, in order to log in from the new device. Enabling Two Step Login helps to prevent account takeover/hijacking if your user-id and password are compromised.

Cryptographic Libraries

SendSafely uses open standards for all cryptographic operations, and relies on the following trusted third-party libraries for encryption-related code:

- Bouncy Castle
  Used by our .NET and Java APIs for OpenPGP support
- Google Keyczar
  Used by our servers to encrypt data at rest, security-related cookies, and other sensitive parameters
- Stanford Javascript Crypto Library
  Used by our front-end web site, JavaScript API and Chrome Extension for certain cryptographic operations
- OpenPGP JS
  Used by our JavaScript API and Chrome Extension for OpenPGP support

Web Application Security

In addition to the encryption mechanisms described above, all communications between the SendSafely servers and your web browser or mobile application are encrypted using HTTPS/TLS (Transport Layer Security). The use of HTTPS/TLS provides an additional layer of encryption on top of the end-to-end encryption already used for file and messages, and is used to safeguard client-server communications and mitigate man-in-the-middle attacks. The HTTP Strict Transport Security header is used across our site to prevent anyone from attempting to fool your browser into making requests to our site that to not use HTTPS/TLS. We also maintain an A+ rating from SSL Labs.

To protect users from cross-site scripting attacks (XSS), SendSafely's web application uses the Content Security Policy standard to declare approved sources of content that are allowed to run within the web application. Only approved sources of client-side code are permitted, so unauthorized attempts to inject JavaScript script into our application will be blocked.

Privacy, Anonymity and Metadata

SendSafely protects the contents of the files and messages you exchange, however SendSafely is not designed to be an anonymous system. Our goal is to keep your data private while providing all of the core features you expect. Our servers have no knowledge of your message contents, but we do store things like your email address, phone number, contacts, and file names. SendSafely also stores additional data such as the time you logged-in, who you send items to, and the IP address you use to access the site. SendSafely will never disclose any of this information or share it with third parties, except when needed in order to fulfill our operations.

Vulnerability Testing

Our engineering team has strong security-related background and experience, however we know that no system is perfect. In order to identify potential security issues, we perform internal security audits on a regular basis and operate a public Bug Bounty Program. Additionally, we have partnered with edgescan for continuous external vulnerability scanning of our systems.

If you think you've identified a security issue please submit the details to us using our Security Bug Reporting Form. Our team will work with you to verify the issue and make sure it gets corrected quickly.

DigitalOcean Cyber Structure and Policies

Physical Security

Our datacenters are co-located in some of the most respected datacenter facility providers in the world. We leverage all of the capabilities of these providers including physical security and environmental controls to secure our infrastructure from physical threat or impact. Each site is staffed 24/7/365 with on-site physical security to protect against unauthorized entry. Security controls provided by our datacenter facilities includes but is not limited to:

- 24/7 Physical security guard services
- Physical entry restrictions to the property and the facility
- Physical entry restrictions to our co-located datacenter within the facility
- Full CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Facilities are unmarked as to not draw attention from the outside
- Battery and generator backup
- Generator fuel carrier redundancy
- Secure loading zones for delivery of equipment

Infrastructure Security

DigitalOcean's infrastructure is secured through a defense-in-depth layered approach. Access to the management network infrastructure is provided through multi-factor authentication points which restrict network-level access to infrastructure based on job function utilizing the principle of least privilege. All access to the ingress points are closely monitored, and are subject to stringent change control mechanisms.

Systems are protected through key-based authentication and access is limited by Role-Based Access Control (RBAC). RBAC ensures that only the users who require access to a system are able to login. We consider any system which houses customer data that we collect, or systems which house the data customers store with us to be of the highest sensitivity. As such, access to these systems is extremely limited and closely monitored.

Additionally, hard drives and infrastructure are securely erased before being decommissioned or reused to ensure that your data remains secure.

Access Logging

Systems controlling the management network at DigitalOcean log to our centralized logging environment to allow for performance and security monitoring. Our logging includes system actions as well as the logins and commands issued by our system administrators.

Security Monitoring

DigitalOcean's Security team utilizes monitoring and analytics capabilities to identify potentially malicious activity within our infrastructure. User and system behaviors are monitored for suspicious activity, and investigations are performed following our incident reporting and response procedures.

Droplet Security & Employee Access

The security and data integrity of customer Droplets is of the utmost importance at DigitalOcean. As a result, our technical support staff do not have access to the backend hypervisors where virtual servers reside nor direct access to the NAS/SAN storage systems where snapshots and backup images reside. Only select engineering teams have direct access to the backend hypervisors based on their role.

Snapshot and Backup Security

Snapshots and Backups are stored on an internal non-publicly visible network on NAS/SAN servers. Customers can directly manage the regions where their snapshots and backups exist which allows the customer to control where their data resides within our datacenters for security and compliance purposes.