CYPHER.DOG®

Cypherdog Encryption

for Legal Services

Encrypt any file, any text, and share via any medium, any time

Opportunities of Encryption in the Legal Profession

When it comes to encryption, the legal profession has a number of opportunities:

- **Secure File Protection:** The use of encryption in the legal field provides attorneys and law firms with a secure platform to store confidential client information and documents. Encryption can be used to encrypt confidential digital files, ensuring the security of client data from unauthorized access. It also ensures that only authorized personnel have access to sensitive documents, thus protecting the integrity of the legal process.

- **Data Integrity & Confidentiality:** By implementing encryption technology in their practice, attorneys can guarantee that any transmitted data is kept safe from malicious attacks and manipulation. Additionally, encryption helps protect confidential communications between attorneys and other parties involved in legal proceedings while enabling them to maintain the trust of their clients.

- **Enhanced Privacy:** In this day and age, where cyber-attacks are becoming more frequent, lawyers need to take extra precautions when handling sensitive client information. Through encryption, they can ensure that their client's data is not exposed or leaked online as well as keep certain conversations private if needed.

- **Reduced Risk of Fraudulent Actions:** Encryption can help reduce the risk of fraudulent actions being conducted against a law firm or its clients by providing an additional layer of security for digital files stored on computers or sent over networks. By using encrypted communications, substantial financial losses can be avoided due to fraudulent activities conducted by a third party.

- **Improved Efficiency:** With the use of encryption technology, lawyers no longer have to worry about wasting time manually locking up all sensitive documents which becomes tedious and inefficient in the long run. This further enhances efficiency in both administrative tasks within a firm as well as during legal proceedings with multiple parties involved at once who could each benefit from this secure communication tool such as virtual meetings between counsels or video conferencing with witnesses etc.

- **Cross-Jurisdictional Compliance:** Through encrypted communications and data storage, law firms are also able to adhere to jurisdictional requirements that may require certain levels of privacy for both local as well as international clients across different countries with varying privacy laws which would otherwise be difficult to maintain without having encryption technology in place.

- **Cost Savings:** Implementing strong encryption practices can greatly reduce costs associated with proper document storage while also eliminating paper waste – thereby helping law firms save money while still adhering to industry standards for data security measures when handling sensitive client information.

- **Increased Security Measures for Remote Working:** As more law firms embrace remote working options, utilizing various types of encryption technology can provide increased layers of protection for both digital assets as well as physical assets stored at home offices – safeguarding important documents from phishing scams, cybersecurity breaches, hacking attempts, etc.

What type of data does your company process?

1. You store and send different documents and e-mails to your consumers: agreements, pleadings and litigation materials, drafts of corporate resolutions, scans of documents and evidence, voice and video recordings, minutes of hearings, and court sessions.
2. You exchange documents and e-mails internally - especially customer documents mentioned above, your corporate documents, financial statements, employee records, contracts and alike.
3. You send typical business documents to your leads & customers such as offers and invoices.
4. You cooperate and exchange different types of documents with an external accounting office, your auditor, bank, insurance broker, and others.

Why should you protect yourself and your customer?

1. Avoid espionage from hackers acting on behalf of competitors or independently looking for customers to buy your data. Data leaks of customer documents can destroy all your hard work and reputation.
2. Avoid data leaks - when everybody can know about your customer documents, litigation materials, pleadings, and evidence.
3. Avoid invoice hacking - when your customer paid to the wrong bank account based on a fake invoice.
4. Avoid ransomware with double extortion when data from your notebooks, e-mail, and servers gets stolen, and you are blackmailed and forced to pay a ransom.

What can happen after a cybersecurity incident?

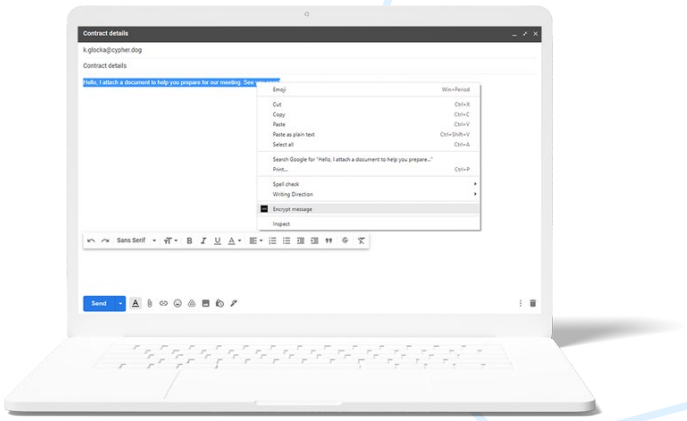
1. You can lose lawsuits because your opponents will know your steps, evidence, strategy, testimony, statements ...
2. Many threads related to your clients' affairs could be used to blackmail or intimidate witnesses or clients
3. You will lose the trust of customers after a data leak. The customers might want to file a case against you.
4. You will damage your reputation as a lawyer.
5. You might have to pay financial penalties to the regulators (GDPR, DORA, NIS-2, Privacy Acts, and others).

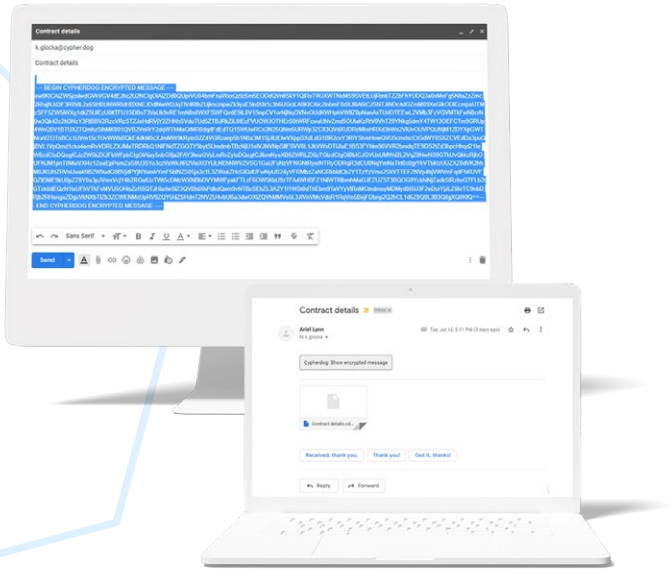
How it works

One-click. Complete protection. Cypherdog Encryption allows you to encrypt and decrypt any text or file and send them using any media, including e-mails supported by plugins to **Firefox, Chrome and Edge browsers, Gmail/Google Suite, Addins in Outlook and Thunderbird.**

You can send and receive encrypted files and messages using any web client or native e-mail client or Slack, WeTransfer, Google Drive, or any other communication method.

You are always assured that only the authorized recipient will have access to the decrypted content.





Threats in cyberspace

E-mail is one of the most popular electronic communication channels. Like most digital services, it is vulnerable to cyberattacks, which may result in **unwanted access** to your mailbox and **disclosure of confidential information**. In the event of unauthorized use of the compromised e-mail box, message recipients cannot verify the sender's identity.

Cypherdog is a **comprehensive solution** to both threats. On the one hand, it ensures message encryption (hiding the content from unauthorized users); on the other hand, it allows the recipient to verify the sender's identity.

We protect you against

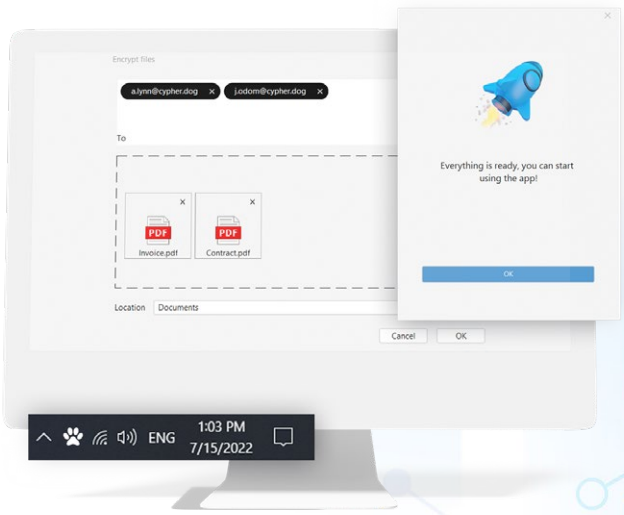
- corporate espionage
- data leaks
- new generation of ransomware with double extorsion
- invoice hacking
- business e-mail compromise (#BEC)

We support you in becoming compliant with GDPR, Privacy Acts, DORA-2, NIS-2, and ISO 2700x implementations, among other regulations.

Friendly user interface

Cypherdog software focuses on simplicity and ease of use. During installation, the program will ask for the **password to your private key** and will allow you to **make a backup** of it (use a USB drive or print a copy of the key on a piece of paper, in the Business version backup is made automatically on company's server). After the installation is complete, **you can encrypt messages and send them via your e-mail immediately.**

macOS



Asymmetric encryption

Absolute protection of private key

No "trusted" third party

Zero-knowledge security model

No service provider access to data

Lack of metadata & logs

Identity trust methods

Cypherdog Encryption specifications	Free (after Trial)	Single User & Trial	Business
Text/e-mail messages encryption	-	x	x
Encryption of files/attachments in e-mail messages	-	x	x
Decryption of e-mail messages/ texts and attachments/ files	x	x	x
Administration panel for users & private keys management	-	-	x
Backup private key to file (on device)	x	x	-
Backup of private key to company server in Vault	-	-	x
One license for a single user	x	x	-
One license for multiple users	-	-	x
Basic support and online training	x	x	-
Advanced support and training	-	-	x
E-mail aliases	x	x	-
Cryptography	Encryption: asymmetric RSA3072 and symmetric AES-256, SHA512 hash function		
Microsoft Outlook	Add-ins to Outlook 2016+ for Microsoft 365/ Exchange Server, webclient & native		
Gmail & Google Suite	Plugins: Google Chrome, Microsoft Edge, Mozilla Firefox		
Mozilla Thunderbird	Add-ons for Thunderbird for all e-mail providers and servers		
Other e-mail clients	Manual encryption / decryption / right-click or "magic window"		
Other communication channels	WeTransfer, Slack, Google Drive, Dropbox, WhatsApp, Messenger etc.		
Operating systems	Windows, macOS, Linux		

CYPHER.DOG®

Cypherdog Security Inc., 100 Wilshire Blvd., Suite 700, Santa Monica, 90401 CA, USA
www.cypher.dog | info@cypher.dog