

Cypherdog Encryption

for Trade & Logistics

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

What type of data does your company process?

1. You send and store different documents and e-mails to your consumers: offers, agreements, order templates, and invoices.
2. You exchange different document types and e-mails with your suppliers with offers, agreements, order templates, and invoices.
3. You cooperate and exchange documents with law firms, HR agencies, external accounting offices, auditors, banks, insurance brokers, marketing agencies, and others.
4. You exchange documents and e-mails internally such as corporate resolutions, financial statements, employee records, contracts, offers during preparation, and drafts of orders.

Why should you protect yourself and your customer?

1. Avoid corporate espionage - especially offers, agreements, and lists of customers - as a result of hackers acting on behalf of competitors or independently looking for customers for your data.
2. Avoid invoice hacking - when your customer paid into the wrong bank account based on a fake invoice.
3. Avoid data leaks - when everybody could know about your business strategy, prices, offer, plans, and databases of customers.
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 will lose your time and money because you lost your deals.
2. You will lose your customers and business opportunities because someone else knows about your price levels, offers, and conditions of contracts.
3. You might lose your customer if it was the victim of invoice hacking. Often the customer will file a case against your business..
4. You might lose the trust of customers after a data leak. Sometimes, you should expect litigation to follow such an incident.
5. You might have to pay financial penalties to the regulators (GDPR, DORA, NIS-2, Privacy Acts, and others).

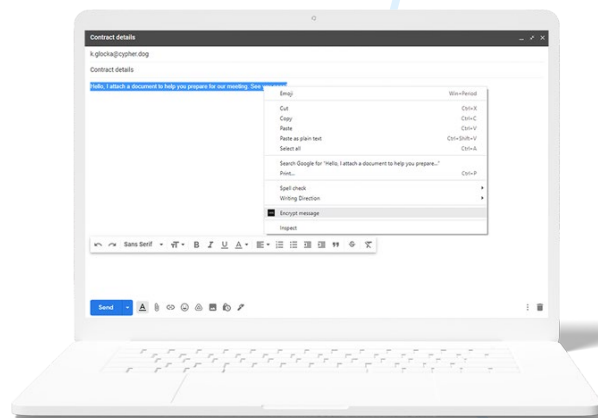


How it works

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.

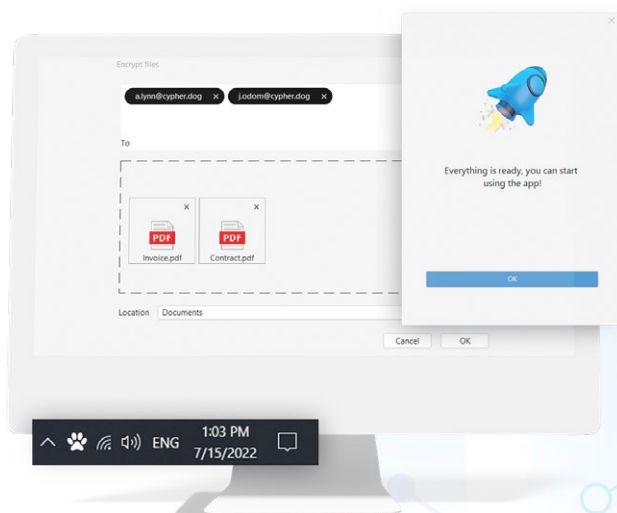
We protect you against

- corporate espionage
- data leaks
- new generation of ransomware with double extortion
- 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.**





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

