CYPHER.DOG®

Cypherdog Encryption

for Financial Services

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

Data privacy and security are the top priority for financial institutions, as well as their customers. As a result, encryption technology has become increasingly important in the finance industry to protect customer information from cyber threats. It is not only used to secure data that is transmitted across networks but also stored on computers and mobile devices. Encryption helps to ensure that confidential data remains confidential by making it unreadable without proper authorization or access keys.

Encryption technology can be used in a variety of ways within the finance industry, such as protecting online banking transactions, preventing credit card fraud, verifying digital signatures when transferring funds between accounts, and more.

This makes encryption an essential tool for safeguarding sensitive financial information from malicious actors who could use it for their own gain or cause harm to customers. Additionally, using encryption can help companies comply with regulations like GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act).

Enhanced Security

Encryption is essential for providing an extra layer of security to financial data. It prevents potential hackers from accessing and exploiting sensitive customer information, such as transaction histories, credit card numbers, bank account numbers, and passwords.

By using encryption, financial institutions can ensure that their customers' personal data is kept safe and secure while they are engaging in digital transactions.

Improved Data Integrity

The use of encryption also helps to protect the integrity of finance industry data by preventing unauthorized access or manipulation. As the data is encrypted, it is impossible for malicious actors to tamper with or alter the information without the correct decryption keys.

This ensures that the customers receive accurate and up-to-date financial information when they access their accounts online or through other digital channels. And, if the data is encrypted while in transit, it can help protect sensitive financial records from being intercepted by cybercriminals.

Increased Customer Trust

Having effective encryption methods in place gives customers peace of mind knowing that their financial information is being safeguarded from any potential threats.

When customers feel secure about their finances, they are more likely to trust a particular financial institution and engage in transactions with them regularly. This could lead to increased customer loyalty and long-term relationships with banks or other financial services providers.

Imagine the damage done if a customer's financial information were to be stolen or manipulated. The reputation of the company would likely suffer, and customers may no longer feel comfortable using their services.

Streamlined Transactions

Encryption also helps streamline digital transactions by ensuring that each message sent between two parties is authenticated and verified quickly and securely before it is approved for completion.

This means that payments can be completed faster without any risk of fraud or misuse of funds due to authentication checks being carried out automatically on both ends of the transaction process.

Reduced Fraudulent Activity

By encrypting all customer data, financial institutions can reduce the chances of fraudulent activities taking place within their systems since it will be much harder for hackers to access this type of information without using sophisticated decryption methods firstly.

This will help keep customers' money safe while also reducing costs associated with having to investigate fraudulent activities after they have occurred due to inadequate security measures being in place beforehand.

And with that, it is clear why encryption has become such an important asset in the finance industry. Not only does it provide increased security, improved data integrity, and trust with customers; but also help streamline transactions and reduce fraudulent activities – making it a valuable tool for both financial institutions and their customers.

Improved Disaster Recovery System

In addition, encryption plays an important role in disaster recovery efforts for financial organizations as well as banks by enabling them to restore lost data quickly should any incidents occur involving natural disasters or cyber-attacks taking place on their systems that could cause widespread damage. Otherwise, if no encryption was used prior then it would take a much longer time for restoring backup copies if possible.

For instance, if a financial institution was to suffer from a cyber-attack, they could quickly use their encryption keys to recover all the important customer data that would have been lost otherwise.

Cost Savings

Using encryption technology also enables organizations within the finance sector to save money on infrastructure costs since it reduces reliance on physical servers which tend to be expensive to operate over long periods of time however when encrypted data is stored on cloud-based platforms then there are fewer hardware requirements thus enabling businesses to capitalize advancements technology better lower overall expenses incurred operations.

Enhanced Privacy

Furthermore, encrypted ensures privacy rights for customers who respected these compliance laws and standards set forth by governments even though may not be direct beneficiaries these regulations still provide added layer of protection for individuals who use services offered by industries.

As a result, companies maintain good reputations meeting expectations at both local and international levels thereby increasing the level of trust among clients and stakeholders alike to maintain a competitive edge sustaining business models over a long-term basis too.

What type of data does your company process?

1. You store and exchange different documents and e-mails of your consumers: invoices, financial statements, bank statements, tax returns, agreements, bank guarantees, insurance policies, etc.
2. You exchange documents and e-mails internally - especially customer documents mentioned above, your corporate documents, financial statements, employee records, contracts, etc.
3. You cooperate and exchange different document types with HR agencies, advertising companies, and other suppliers of goods and services.

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 your customer documents can destroy all work and reputation.
2. Avoid data leaks - when everybody can know about your customer documents.
3. 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. Hackers demand ransom for not disclosing stolen data but might do so anyway.
4. Avoid invoice or other documentation hacking - when your customer paid using the wrong wire transfer information based on a fake invoice.

What can happen after a cybersecurity incident?

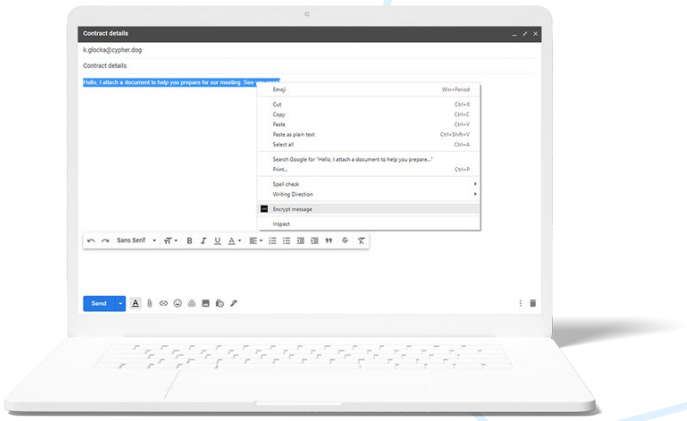
1. You will lose the trust of your customers after a data leak. In tough times, it is not uncommon for competitors to engage in criminal behavior designed to destroy your business.
2. You might have to pay financial penalties to the regulators (GDPR, DORA, NIS-2, Privacy Acts, and others).
3. You will damage your reputation as a company, which can be detrimental to your business.

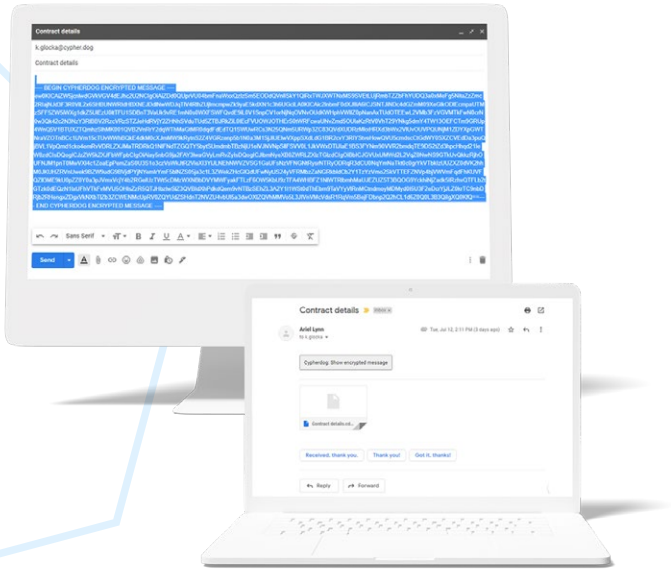
How it works

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

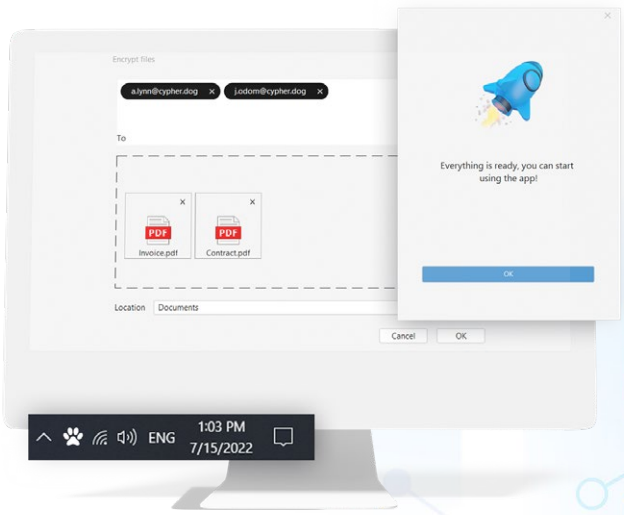
- corporate espionage
- data leaks
- new generation of ransomware with double extorsion
- invoice hacking
- business e-mail compromise (#BEC)

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