CYPHER.DOG®

Cypherdog Encryption

for Manufacturing & Supply Chain

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

Potential Risks of Not Encrypting Data in the Manufacturing Industry

The manufacturing industry relies on the exchange of sensitive information such as financial data, intellectual property, and confidential business plans. If this information falls into the wrong hands, it can have disastrous consequences for the company. Therefore, not encrypting e.g. e-mail in the manufacturing industry can pose several risks, such as data breaches, cyberattacks, and regulatory compliance issues.

To name an example, in 2016, a data breach at a FA-CC exposed the personal information of their employees, including names, social security numbers, and bank account information. The company had failed to properly encrypt its e-mails, which allowed cybercriminals to intercept sensitive information.

How Encryption Can Help Protect Sensitive Information in the Manufacturing Industry

Encryption can help protect sensitive information from unauthorized access and interception by encoding the content so that it can only be read by the intended recipient. It can prevent cybercriminals from intercepting sensitive information and help ensure that confidential data remains private.

Types of Information That Should Be Encrypted in the Manufacturing Industry

Sensitive information that is typically shared via e.g. e-mail in the manufacturing industry should be encrypted. This includes financial data, intellectual property, confidential business plans, and employee and customer personal data. By encrypting this information, manufacturing companies can reduce the risk of data breaches and protect the privacy of their employees and customers.

How Encryption Can Help Manufacturing Companies Comply with Data Protection Regulations

Encryption can help manufacturing companies comply with data protection regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These regulations require companies to protect the personal data of their customers and employees and can impose significant fines and penalties for non-compliance. By encrypting content containing personal data, manufacturing companies can reduce the risk of non-compliance and protect their customers' and employees' personal data.

Common Methods of Encryption Used in the Manufacturing Industry

There are several encryption methods used in the manufacturing industry, including end-to-end encryption, S/MIME, and PGP. End-to-end encryption is a method where the e-mail is encrypted before it leaves the sender's device and can only be decrypted by the intended recipient. S/MIME and PGP are encryption protocols that use public and private keys to encrypt and decrypt e-mails.

Ensuring Encryption Methods Are Secure in the Manufacturing Industry

Manufacturing companies should take steps to ensure that their data encryption methods are secure. This includes choosing reliable e-mail encryption software and training employees on best practices. Choosing a reputable software provider with a proven track record of security can help ensure that the important information is properly encrypted and protected. Training employees on best practices can help prevent common errors such as sending unencrypted e-mails or using weak passwords.

Impact of Encryption on Productivity and Efficiency in the Manufacturing Industry

Some manufacturing companies may worry that encryption will slow down their productivity and efficiency. However, encryption can increase productivity and efficiency by reducing the time and effort needed to address data breaches and cyberattacks. By implementing encryption software, manufacturing companies can prevent these incidents from occurring in the first place, allowing them to focus on their core business activities.

Training Employees on Encryption Best Practices in the Manufacturing Industry

To ensure that encryption is effective, manufacturing companies must train their employees on email encryption best practices. This includes teaching employees how to use encryption software correctly, how to create strong passwords, and how to identify and report suspicious e-mails. By educating employees on best practices, manufacturing companies can reduce the risk of human error and prevent cyberattacks.

How Encryption Can Help Protect Against Cyberattacks in the Manufacturing Industry

Encryption can help protect against cyberattacks in the manufacturing industry in several ways:

Protecting sensitive information: Manufacturing companies often handle sensitive information such as intellectual property, trade secrets, and customer data. Encryption ensures that this information is protected from cybercriminals who may steal data.

Preventing phishing attacks: Phishing is a common tactic used by cybercriminals to trick employees into revealing sensitive information or downloading malware. Encryption can help prevent phishing attacks by ensuring that only authorized recipients can access the encrypted informations or files.

Securing e-mail attachments: Cybercriminals often use e-mail attachments to spread malware or gain unauthorized access to systems. E-mail encryption can help protect against these types of attacks by securing e-mail attachments with strong encryption.

Enhancing authentication: Encryption can also enhance authentication by using digital signatures and certificates to verify the identity of the sender and recipient. This helps prevent spoofing and ensures that sensitive information is only sent to authorized individuals.

Complying with regulations: Manufacturing companies are often subject to data protection regulations such as the GDPR and the CCPA. Encryption can help these companies comply with these regulations by ensuring that sensitive information is protected during transmission.

Overall, encryption is an essential security measure that can help protect against cyberattacks. By implementing strong encryption protocols, manufacturing companies can ensure that their sensitive information is protected and that their systems remain secure.

What data does your company process?

1. You send and store documents with your intellectual property such as technology and project details.
2. You send and store different documents and e-mails to your consumers: offers, agreements, order templates, and invoices.
3. You exchange different documents and e-mails with your suppliers with offers, agreements, order templates, and invoices.
4. You cooperate and exchange documents with law firms, HR agencies, external accounting offices, auditors, banks, insurance brokers, marketing agencies, and others.
5. 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 that of intellectual property. This also includes offers, contracts, and lists of customers. Hackers act on behalf of competitors or are independently looking for customers to buy 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 can 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?

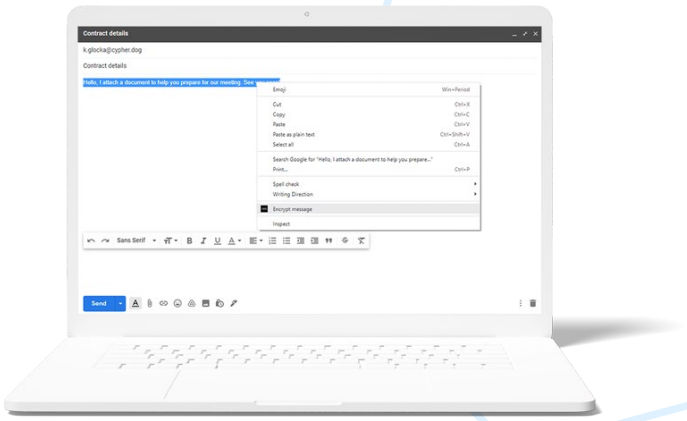
1. You will lose your time and money because of the theft of your competitive advantage and deals.
2. You will lose your customers and business opportunities because someone else knows about your price levels, offers, and conditions of contracts.
3. You will lose the trust of your customers after a data leak. Sometimes litigation wil follow as a result of the incident.
4. You might lose your customer if they were a victim of invoice hacking. Often the customer will commence civil proceedings.
5. You might have to pay financial penalties to the regulators (GDPR, DORA, NIS-2, Privacy Acts, and others).

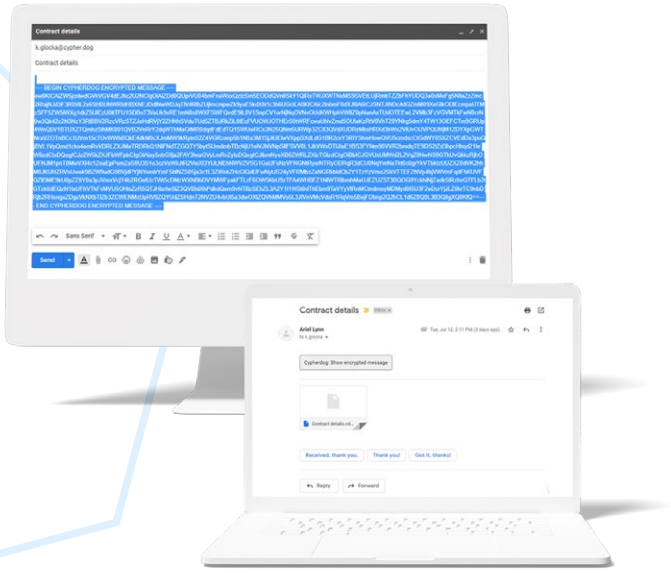
How it works

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

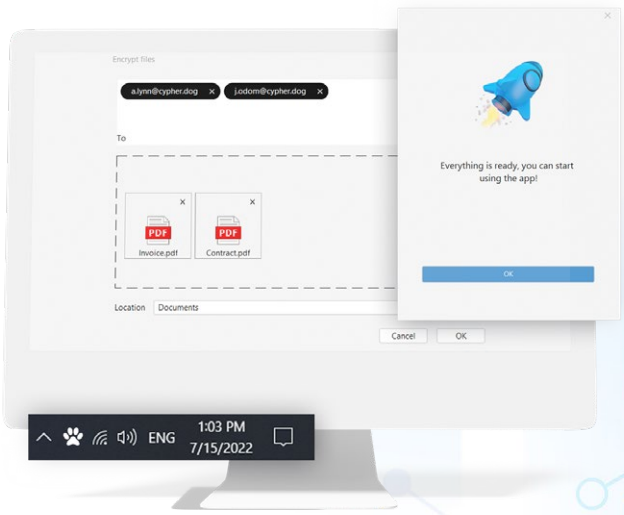
- corporate espionage
- data leaks
- new generation of ransomware with double extorsion
- invoice hacking
- business e-mail compromise (#BEC)

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