inlockly

Causes and Effects of a Potential Data Breach in Your Company

How to Protect a Company from Financial Losses Caused by the Leakage of Access Passwords, Payment Cards, and Other Confidential Data Due to a Cyberattack?



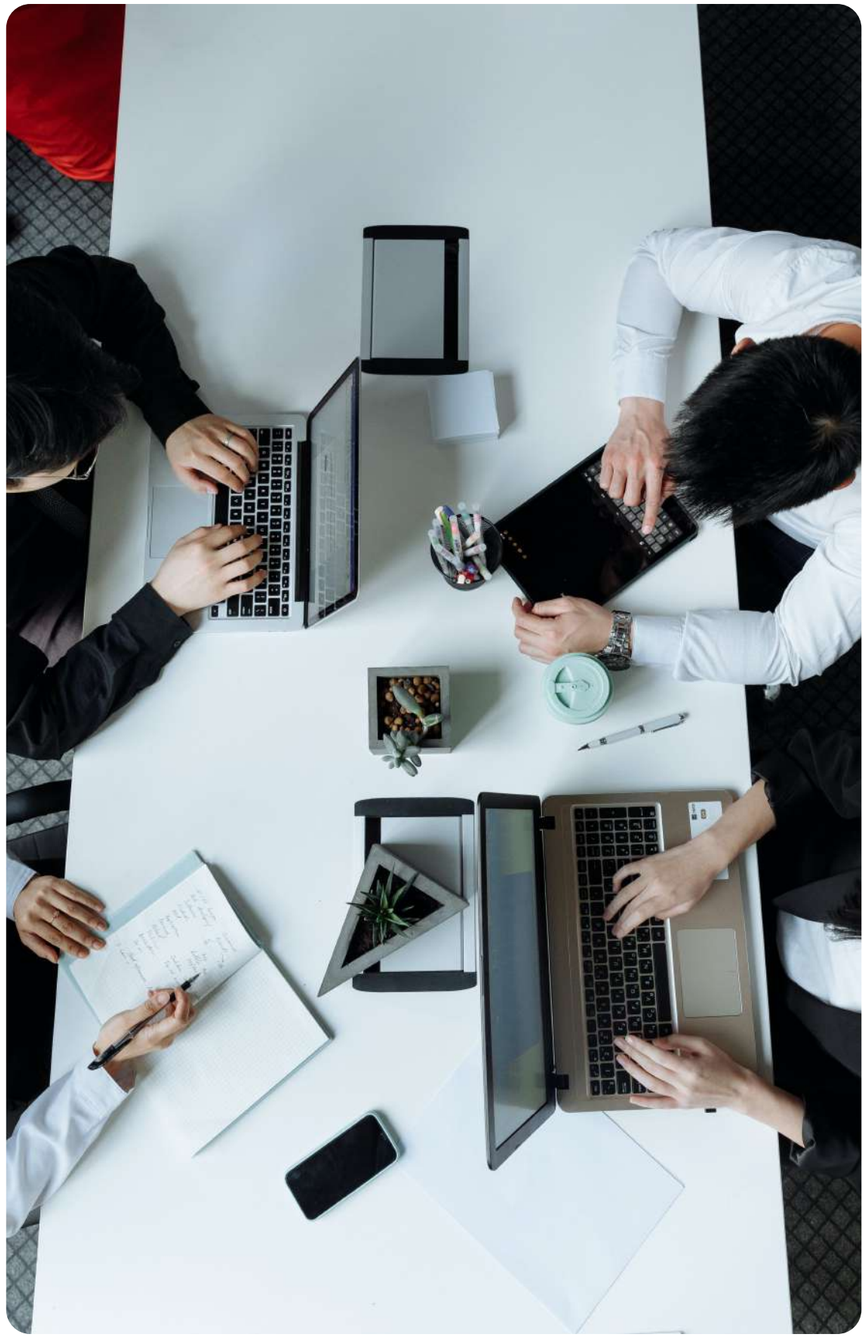
www.inlockly.com

Introduction

Ladies and Gentlemen,
Today, we will address an issue that is becoming increasingly critical for the functioning of every company—namely, **data security**.
The protection of information is essential for the success and integrity of any enterprise. In today's presentation, we will focus on the potential causes and consequences of data breaches in various companies.

Let us begin with a brief visualization. Imagine the following scenario: a data breach occurs in our company. What could be the potential consequences of such an incident? The loss of confidential information, such as passwords, payment card details, or other sensitive data, could pose a serious threat to the company's financial stability. This is not only about the loss of data but also about the impact on the trust of customers and business partners.

The following material aims to provide a deeper understanding of the factors leading to data breaches in a business context and an analysis of the potential consequences. We will also present a tool that can be implemented to minimize risks and enhance the protection of your enterprise.



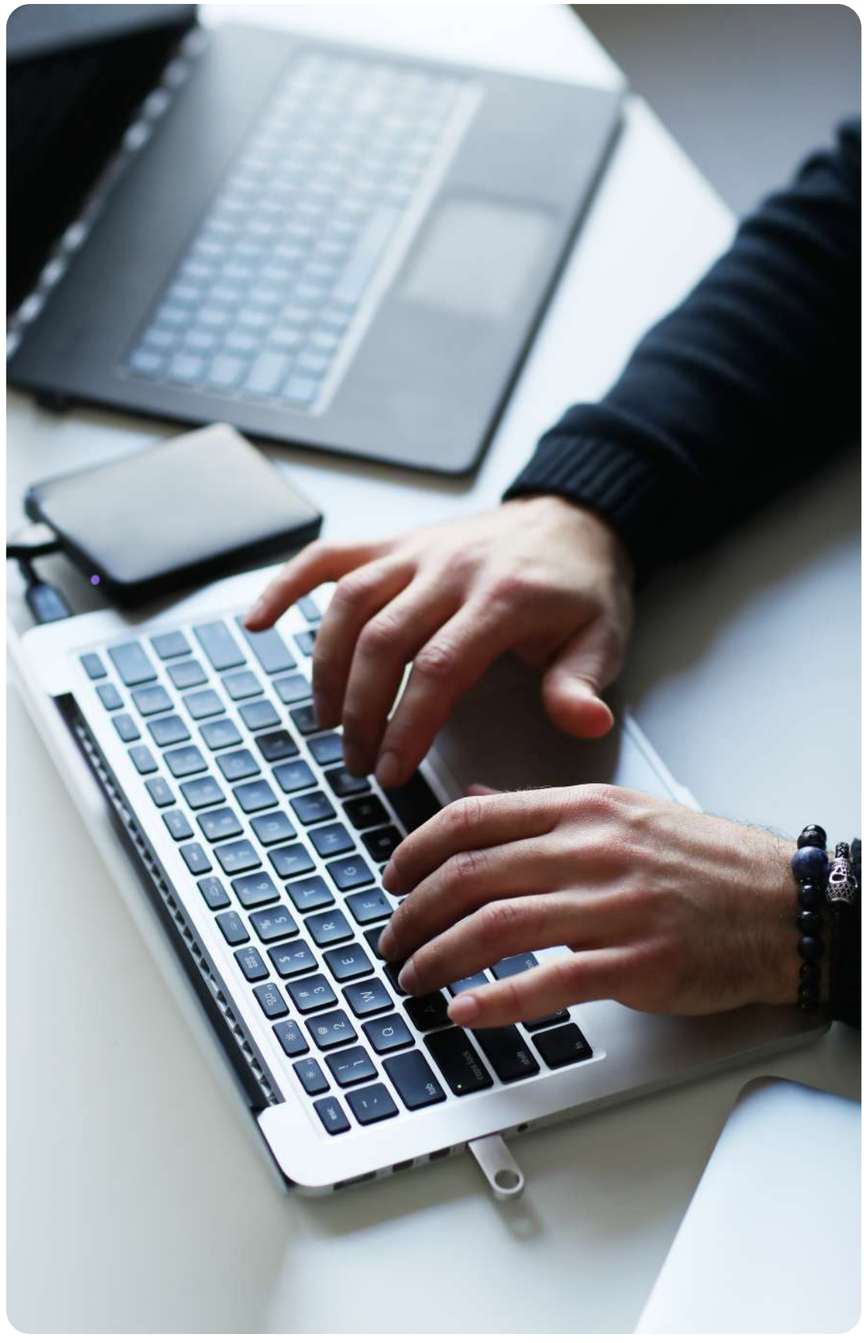
With kind regards,
The inlockly.com Team

Which companies are vulnerable to cyberattacks?

Companies vulnerable to attacks.

Cybersecurity is an integral part of reality for businesses, regardless of their industry or size. Modern threats from attacks affect almost every entrepreneur, regardless of the nature of their operations. Explore methods to enhance your company's level of security in cyberspace.

70% of companies have encountered situations that threatened the security of their data and IT systems. At the same time, business owners themselves rate their cybersecurity resilience as low.



The increase in the risk of cyberattacks in recent years.

In recent years, we have observed an alarming increase in the risk associated with cyberattacks. The dynamic development of technology and global digitization are making businesses increasingly vulnerable to cyberattacks. In this context, it is important to examine the factors that have contributed to this rise in risk over the past few years and to understand the challenges that today's cyberspace realities present to us.

Remote work

The rise of remote and hybrid work practices in recent years has introduced new challenges and dramatically changed the security landscape.
In response to the COVID-19 pandemic, 72% of small businesses worldwide reported that they accelerated their digital transformation projects.

Such rapid adoption of technology has made many small businesses vulnerable to cyber threats. Working from various locations and using different devices, remote employees become potential targets for attacks.

Almost one-third of cybersecurity incidents in small businesses led to data breaches in 2020, and login credentials were compromised in 44% of confirmed breaches.
Remote workplaces require access to confidential company data (including login credentials) from different locations, which demands proper security measures.

Global digitalization

Global digitization, an integral part of modern business, significantly increases the risk of cyberattacks. The widespread adoption of digital technology on a global scale makes businesses from various industries more vulnerable to complex cyber threats.

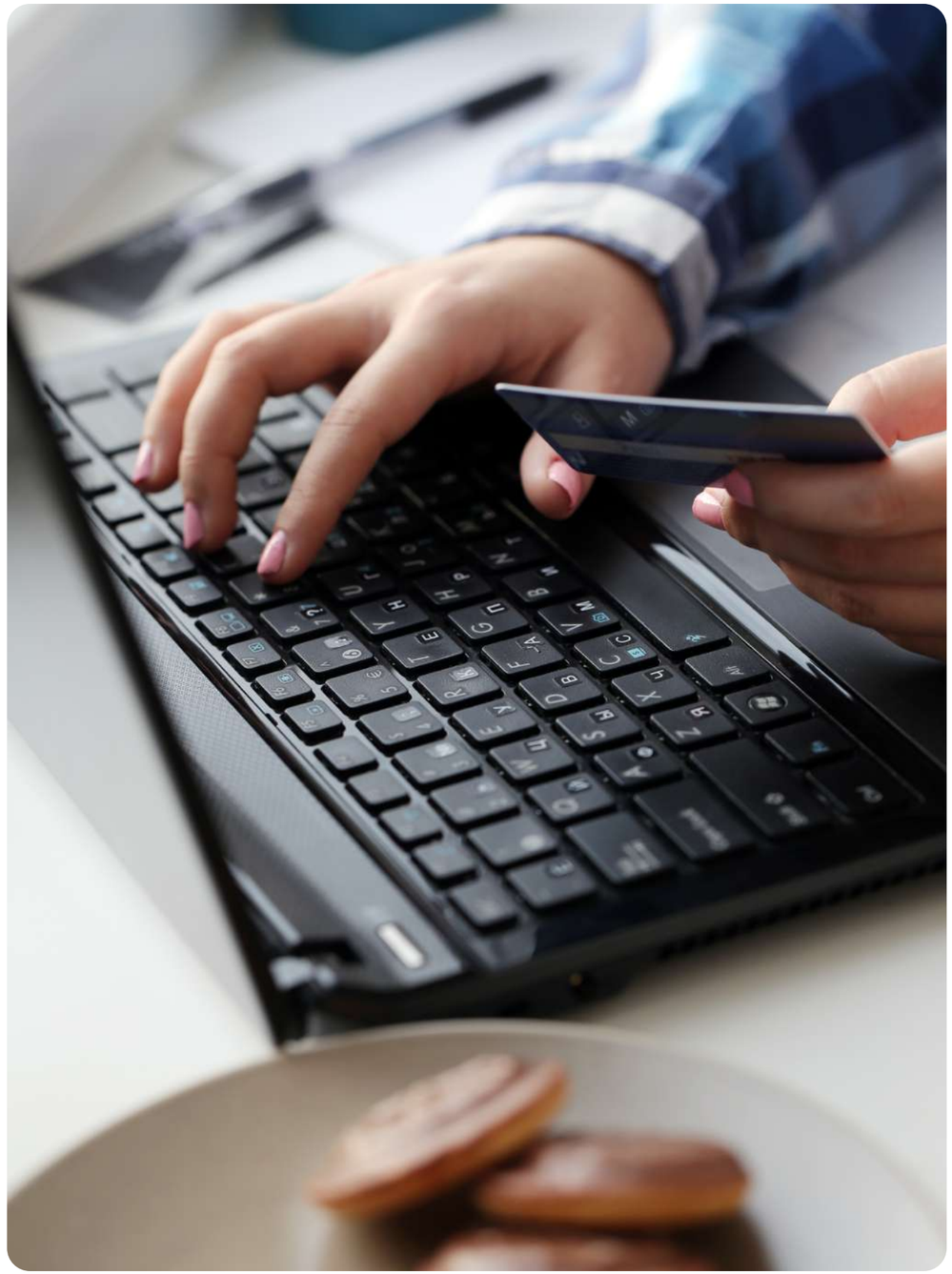
In a world where companies are transitioning to data-driven business models, every organization becomes a potential target for attackers. The growth of online systems, web platforms, and the use of IoT (Internet of Things) technologies creates new points of access that can be exploited by cybercriminals.

In this reality, where data is a key asset, the need for effective protection against cyberattacks becomes imperative for every organization, regardless of its size or industry. Valuable information and confidential data are prime targets for attacks, emphasizing the importance of proper security strategies in the era of global digitization.

Examples of types of attacks causing data breaches in companies.

Phishing

Phishing is a form of cyberattack that involves online fraud aimed at obtaining confidential information from users. The attackers, known as phishers, impersonate a trustworthy source to deceive the victim and gain access to their personal, financial, or other sensitive information.



Basic characteristics of a phishing attack

Identity theft

Phishers often impersonate well-known and trusted institutions, such as banks, companies, government agencies, or online services. Their attacks often appear very authentic.

E-mail messages

One of the common methods of phishing is fake emails. Phishers send emails pretending to come from trusted sources and ask victims to provide confidential information, such as credit card numbers or passwords.

Phishing websites

Phishers create fake websites that mimic legitimate services to convince victims to enter their data. They often use similar URLs or domains to make the sites appear authentic.

Smishing attacks

Smishing is a variant of phishing where attackers use text messages (SMS) for fraud. Victims receive fake messages asking them to provide personal information.

Spear phishing attacks

In the case of spear phishing, attackers focus on specific individuals or organizations. They create more personalized and precise attacks, based on information gathered about their targets.

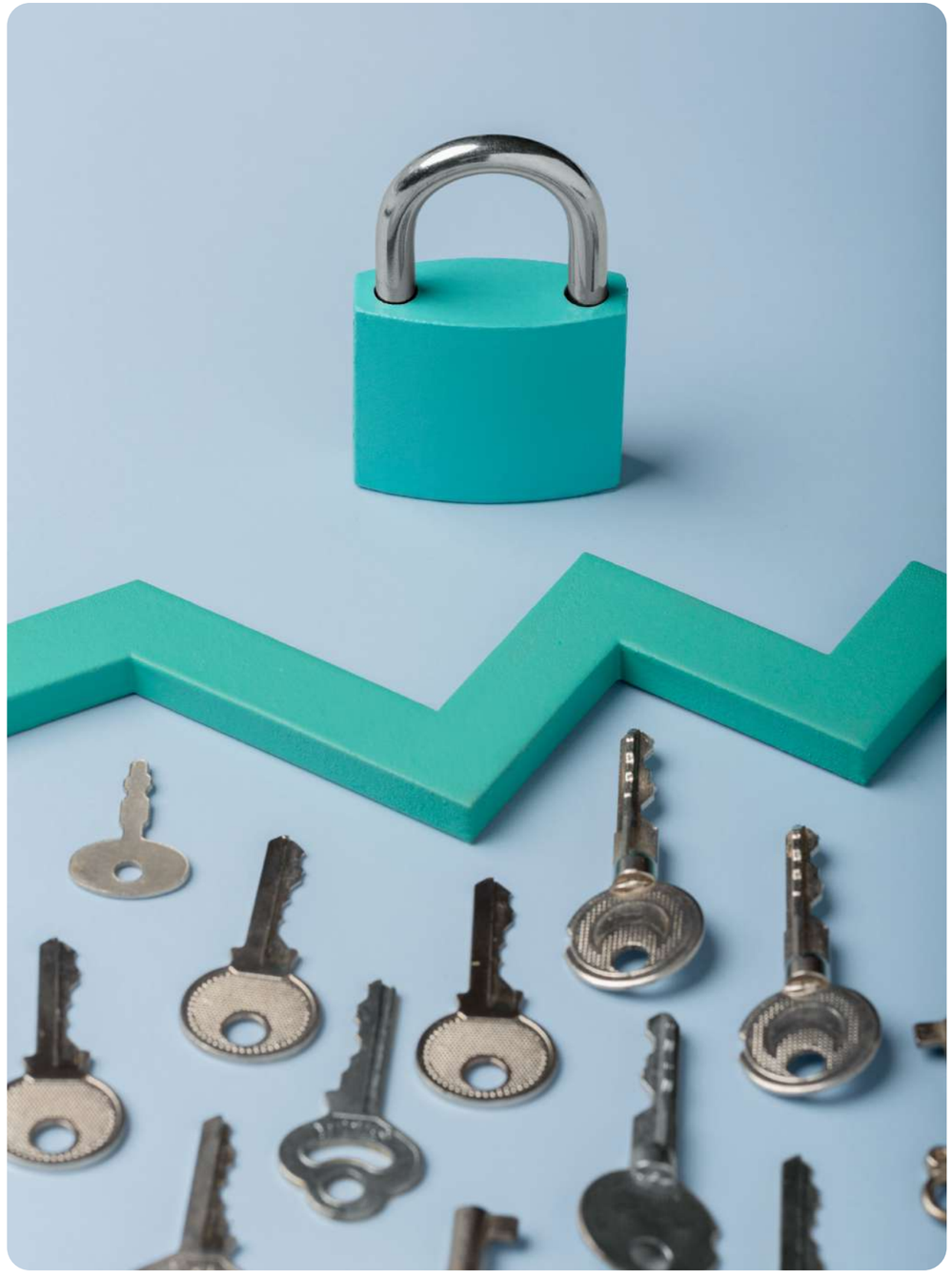
Social engineering attacks

Phishers also use social media to impersonate friends, companies, or institutions. They send links to fake websites, encouraging victims to click and provide confidential information.

To avoid phishing, it is important to exercise caution when opening emails, clicking on links, or sharing confidential information online. User education and the use of additional security measures, such as anti-phishing filters, are crucial for effective protection against this type of cyberattack.

Bruteforce

A brute force attack is a method in which an attacker attempts to gain access to an account or system by repeatedly trying different password combinations. The attacker uses automated programs or scripts that systematically test all possible password combinations until the correct one is found. This is one of the simplest forms of attack, but it can be effective, especially if the user employs weak, easily guessable passwords.



Basic characteristics of a brute force attack

Countless attempts

The attacker attempts multiple login attempts, testing different password combinations to gain access to the account. This method relies on testing all possible combinations.

Use of automatic programs

A brute force attack is often carried out using automated programs that quickly and systematically test various passwords without human involvement.

Weak passwords are easy to crack

This type of attack is particularly effective against weak passwords, such as simple character sequences, dictionary words, or common combinations.

Threat to online accounts

Brute force attacks can be targeted against online accounts, such as email accounts, social media profiles, or even bank accounts.

Increased efficiency with weak security

If the system lacks proper security measures, such as account lockout after several failed attempts, a brute force attack becomes more effective.

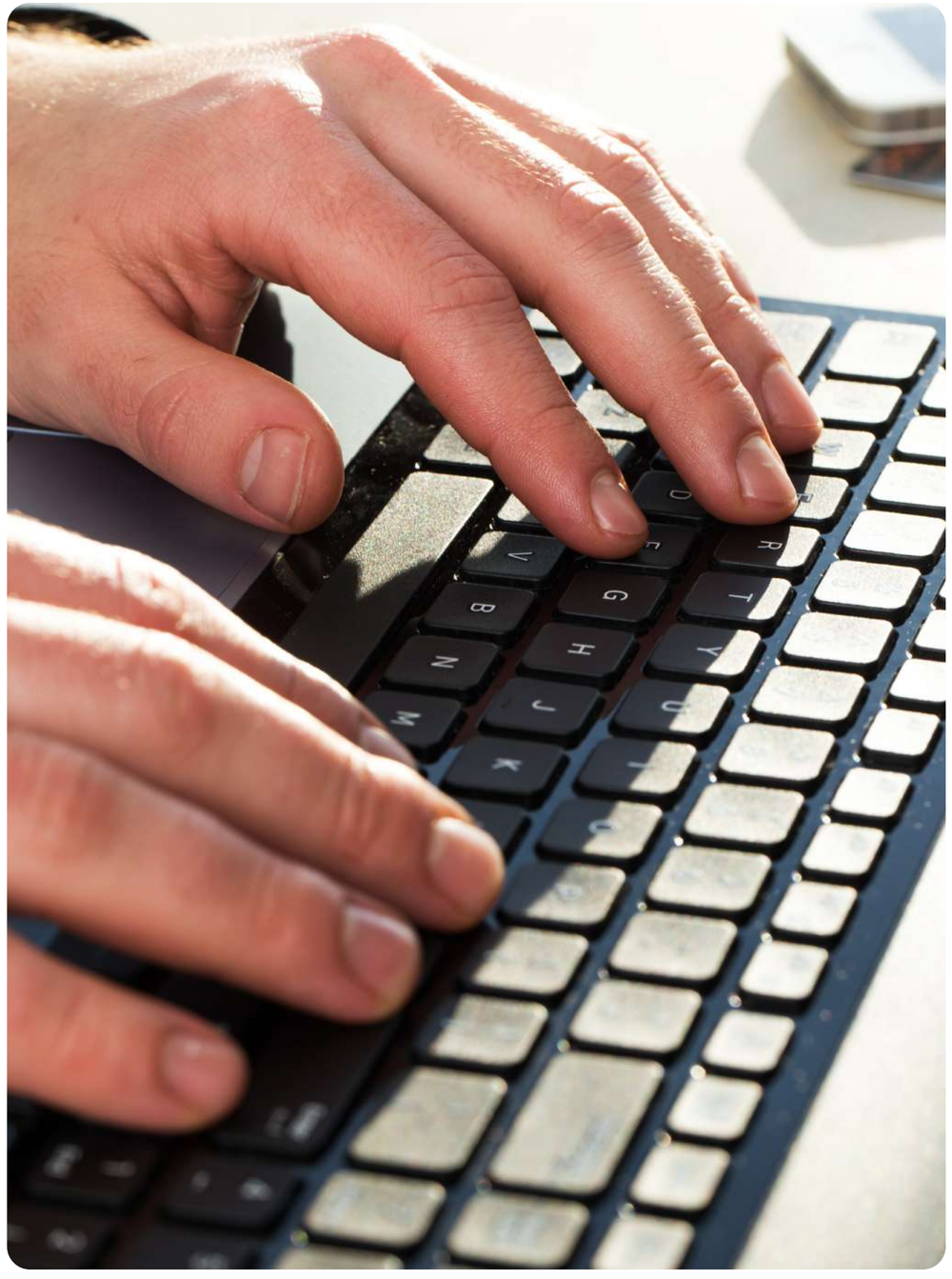
Dictionary Application

A variant of the brute force attack is the dictionary attack, where the attacker tests popular passwords, dictionary words, or combinations of known text.

To effectively protect against brute force attacks, it is important to use strong passwords that are difficult to guess, as well as implement additional security measures. These may include account lockouts after several failed login attempts, the use of multi-factor authentication, activity monitoring to detect suspicious actions, and the use of password managers that help generate and remember unique passwords. User education on secure password practices also plays a crucial role in protecting against such attacks.

Keylogging

A keylogger attack is a cyberattack technique in which malicious software is used to record or monitor the keys typed by the user on a computer or mobile device's keyboard. The purpose of the keylogger is to capture any information entered via the keyboard, such as passwords, login credentials, credit card numbers, or other sensitive information.



Basic characteristics of a keylogger attack

Invisibility for the user

A keylogger operates in stealth mode and is typically invisible to the user. The attacker tries to keep the keylogger running in the background, so the victim is unaware of its presence.

Attacks on computers and mobile devices

Keyloggers can target both desktop computers and mobile devices, which are used to input information via on-screen keyboards.

Targeted attacks on financial data

Keylogger attacks often aim to obtain financial data, such as credit card numbers or banking account information.

Recording all keyboard actions

A keylogger records all keystrokes made by the user, collecting information such as entered passwords, email messages, login credentials, and other text.

Different forms of attack

Keyloggers can take the form of hardware (physical devices connected to the computer) or software (applications running in the operating system).

Remote data transfer

The collected data is often sent to the attacker via the internet. This can occur through email, FTP, HTTP, or other data transmission methods.

Protection against keylogger attacks includes regular antivirus scans, avoiding clicking on suspicious links or attachments, using anti-malware software and password managers, as well as raising user awareness about online threats and security practices. Modern security tools often detect and block keylogger activity, but regular updates and monitoring are crucial to maintaining effective protection.

Other factors that threaten data security

Failure to follow a company password policy

The lack of consistent adherence to password policies creates potential security gaps. Users who employ weak or unchanged password combinations expose the organization to the risk of easy access by potential attackers to various company resources, which could have disastrous consequences for the business.

Insufficient data protection

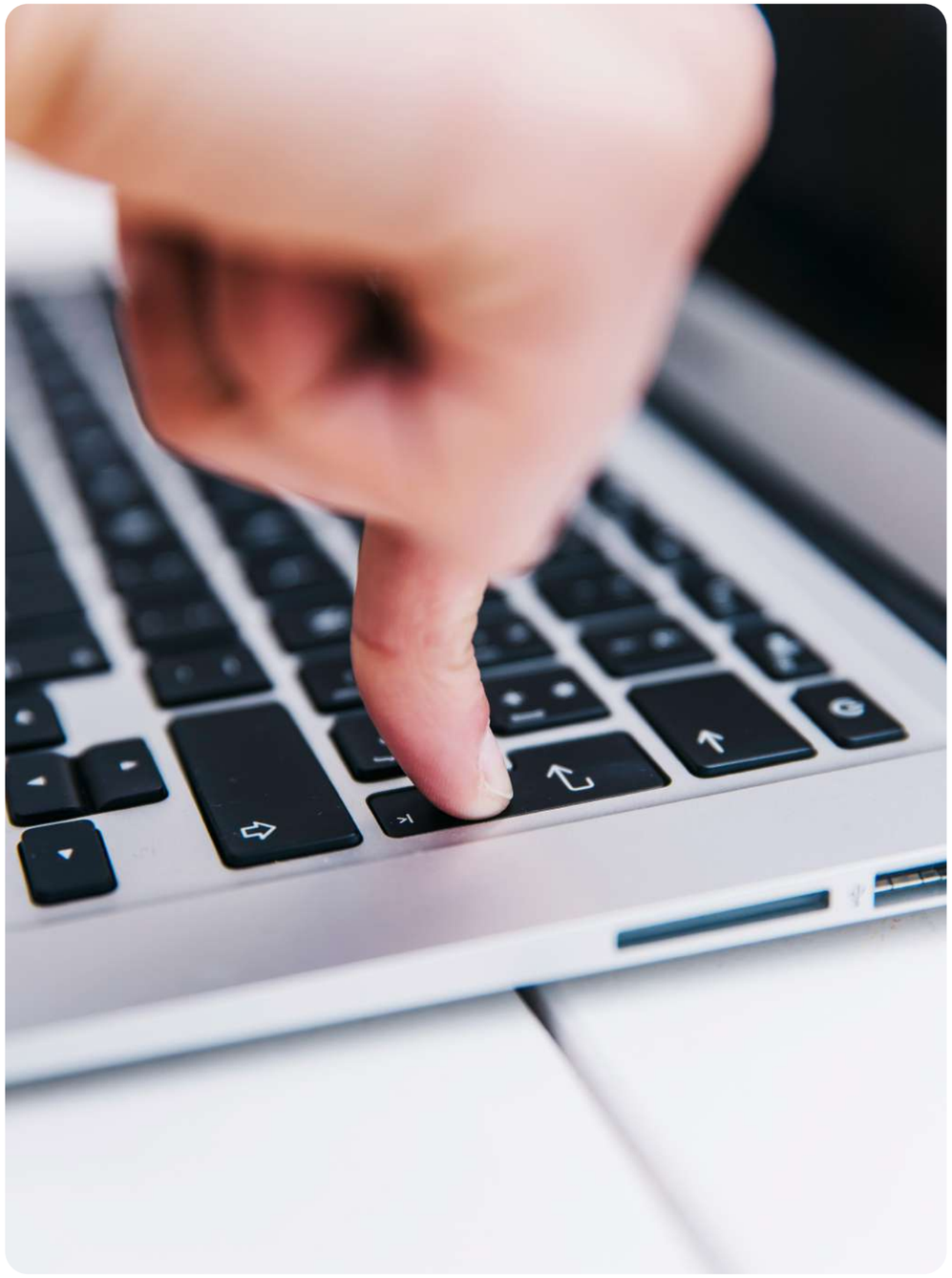
The lack of effective data protection mechanisms, such as encryption and proper access and sharing management, makes company information more vulnerable to theft and unauthorized access.

Lack of appropriate permissions

Excessive access to data for employees who do not need it can lead to abuse. The principle of least privilege involves granting employees only the permissions that are absolutely necessary to perform their daily tasks.

Lack of training for employees

Insufficient cybersecurity training for employees makes them a potential weak link in the defense chain. Unaware employees may make mistakes, such as clicking on suspicious links or opening malicious attachments.



What are the consequences of a data breach in a company?

Main consequences

The first visible effect of cyberattacks is the disruption or paralysis of the normal functions of a business—especially when company owners or employees do not have access to data, such as being unable to log into their email remotely or access files on the cloud.

Sometimes, not all effects of an attack are immediately visible. What should raise concern and suspicion are slow device and application performance, sudden disappearance or appearance of files or folders on a device, as well as the sending of spam from devices (e.g., computer, phone).

A painful and another common consequence of cyberattacks is financial loss for companies:

a. Downtime caused by a cyberattack results in a loss of revenue: data published by NASK indicates that two-thirds of companies that fell victim to a cyberattack experienced a significant decline in revenue related to the incident.

b. The loss or damage of data can also be costly. In many cases, another significant cost is the repair of hardware or infrastructure and the work associated with these repairs.

In the long term, a cyberattack negatively impacts the company's reputation in the market.

Financial losses for companies resulting from data security breach incidents.

The average costs of incidents and breaches for companies in 2020:

Number of employees	Cost
1-9	7 000$
10-49	17 000$
50-249	50 000$
249-999	133 000$
1000+	504 000$

Based on data from eight countries.
Source: Hiscox, "Hiscox Cyber Readiness Report," 2020.

How to mitigate the risk of data breaches in a company?

12 Best Password Management Practices for Employees.

1. Use different and strong passwords for each system and account.
2. Do not use personal information (including pet names or anything that can be guessed from social media) to create passwords.
3. Do not use dictionary words from any language.
4. Use the longest possible passwords, never shorter than 12 characters.
5. Require at least two methods of user identity verification through two-factor authentication (2FA) or multi-factor authentication (MFA) whenever possible.
6. Change the passwords for all accounts affected by a security incident.
7. Do not write down passwords or leave them on your desk or taped to your computer.
8. Do not store passwords in your web browser.
9. Implement a strong corporate policy and enforcement system that prevents the use of weak passwords.
10. Remove accounts and applications that are no longer in use.
11. Change default passwords for critical systems, such as remotely accessible devices or anything that connects to the internet.
12. Do not send colleagues passwords for shared accounts using insecure methods, such as text chats, emails, or notes – always use encrypted sharing, for example, through a password manager.

5 Additional Rules for Administrators.

1. Use encryption when storing or sharing passwords.
2. Implement advanced authentication methods such as 2FA/MFA (e.g., mobile authentication apps or hardware tokens).
3. Change passwords for shared accounts and revoke individual accounts when an employee leaves the company.
4. Add additional security measures for privileged accounts – for example, by implementing an Identity and Access Management (IAM) solution that enforces more stringent policies for these users.
5. Educate employees, contractors, and other users not to reuse corporate passwords for personal accounts.

User access control and management of permissions across departments in the company.

A password manager helps different teams in the company securely perform their work. This versatile tool becomes even more important as the company grows, adding new functional teams and more employees who handle sensitive accounts and information.

Below are some examples of key functional areas that could benefit from better password management.

Sales and customer service

Sales teams access a variety of customer data daily through applications like Customer Relationship Management (CRM) platforms. This data includes personally identifiable information (PII), and your teams must maintain customer trust by protecting this information.

Human Resources (HR)

Employee personal data – such as identification numbers and birthdates – is highly valuable to cybercriminals. As the custodians of this data, Human Resources (HR) teams are often targeted by cyberattacks. Additionally, some HR employees are responsible for onboarding new hires, which means they may manage dozens, or even hundreds, of login credentials. A password manager helps the HR department protect sensitive data and easily onboard employees.

Finances

Depending on the functional structure, the finance department's activities may include basic accounting and bookkeeping tasks, cash flow management, forecasting, and capital raising. These activities give the finance team access to a wide range of critical financial information, which is managed through various accounts and systems, and this information must be protected.

Technology (IT)

A typical small business has a very small IT team, and employees in other roles may share administrative duties. The list of responsibilities is long, including protecting the website from hacks, onboarding and offboarding employees from various applications and other IT resources, handling breaches and intrusions, and resetting passwords. A password manager can streamline all of these tasks while enhancing security and helping establish a security-conscious culture.

Marketing

The marketing and communications team is one of the most prolific users of digital tools. These employees juggle dozens of logins, from social media and content management platforms to graphic design, analytics, and project management applications. Often, these logins are shared insecurely and reused across multiple platforms, which could be hacked if not properly protected.

Payrolls

Payroll employees handle both personal data and financial information for the entire staff. Like the HR team, this critical functional area is often targeted by cybercriminals seeking individuals with privileged access. Employees expect companies to protect this information to the necessary extent.

Orders and suppliers

In addition to employee and customer data, confidential information provided by suppliers must also be protected. These records may include everything from government identification numbers of freelancers to business bank accounts and other sensitive information required during supplier onboarding. By safeguarding this data, the procurement team can maintain the trust of valuable partners.



Our solution – the Inlockly™ app, available on multiple platforms.

GDPR COMPLIANT

CCPA COMPLIANT

What is the Inlockly™ app?

The Inlockly™ app is a password manager tool that stores all your passwords in one secure location, while also allowing easy management of logins and the creation of long, random, and unique passwords. You only need to remember one password – the master password for the Inlockly™ app.

The password manager automatically syncs all passwords across multiple devices, so you can access and manage them from anywhere.

We use the strongest available encryption, enable one-click login to accounts, and offer a range of additional benefits.

How does our app protect against previously known threats?

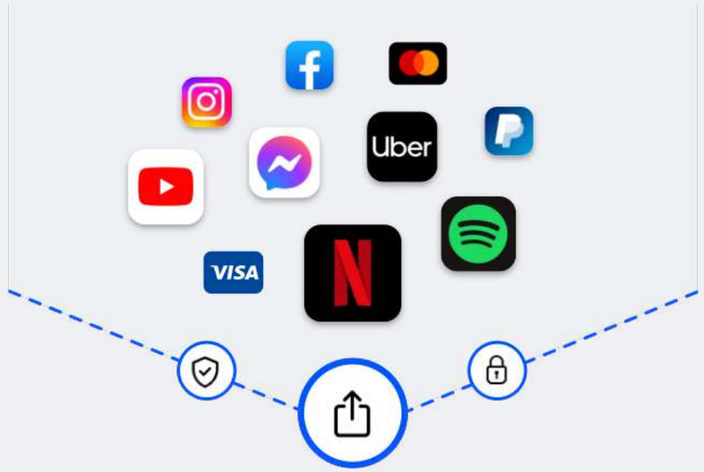
Inlockly™ significantly helps all employees adhere to best practices in password security and access management, reducing the risk of data breaches caused by previously known attacks.

- **Protection against phishing**
- **Protection against keylogging**
- **Protection against brute force attacks**
- **Assistance in enforcing password policy**
- **Secure sharing of employee data**
- **Permission management and access control**

Protection against phishing

Inlockly™ plays a crucial role in protecting against phishing through several key features and practices, such as:





Hiding login data on untrusted websites

The Inlockly™ app automatically fills in login forms on websites. This eliminates the risk of users entering login credentials on fake phishing sites. Login data is strictly tied to the domain address, and these addresses are automatically compared with the one the user is visiting – if they do not match, the data is hidden.

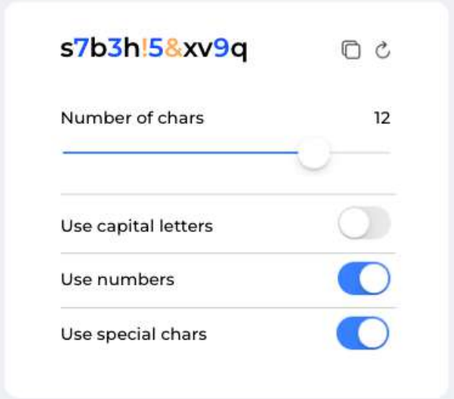
Storing other sensitive data

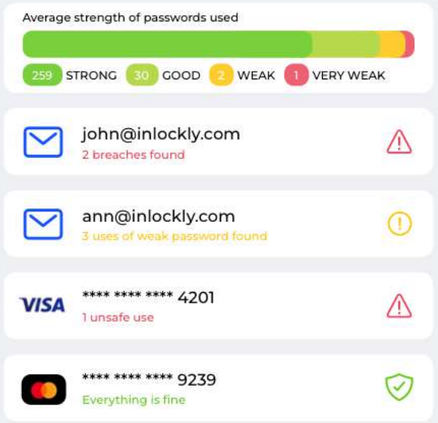
Inlockly™ stores not only passwords but also other sensitive data, such as credit card numbers, business notes, and personal information, all in a secure and encrypted manner.

With its built-in URL filter, the app alerts the user when a website is not trusted, protecting information from leakage during phishing attacks.

Protection against brute force attacks

Inlockly™ protects against brute force attacks through the implementation of several key security mechanisms:





Generating and storing strong and unique passwords

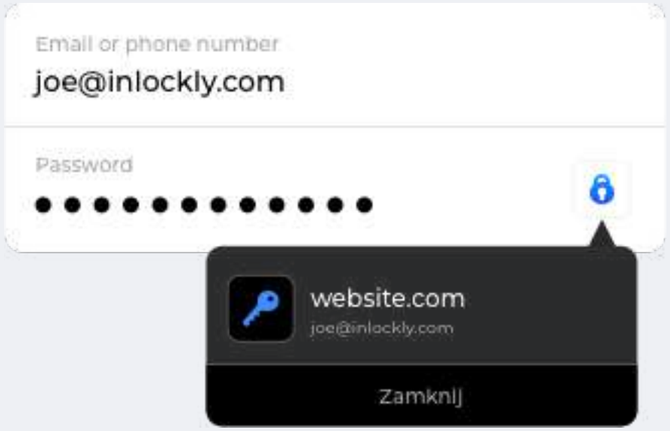
Inlockly™ allows for the generation and storage of strong, random passwords for each account. These passwords are typically long and include a variety of characters, making it significantly more difficult to crack them using brute force attacks. Such phrases are hard to remember without a password manager, which is why Inlockly™ will store them for you and automatically fill them in when attempting to log in to trusted websites.

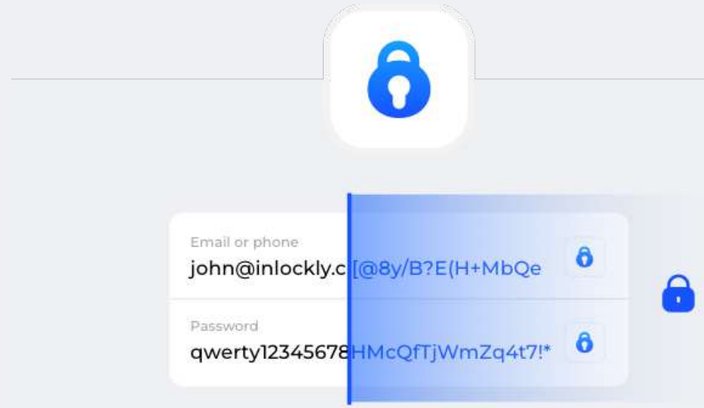
Warnings about weak passwords

Inlockly™ automatically calculates the strength of passwords and warns users about using weak phrases, encouraging them to opt for more secure combinations.

Protection against keylogging

Inlockly™ helps protect against keylogging, which is the recording of keystrokes by malicious software, through the implementation of the following security measure:





Automatic form filling

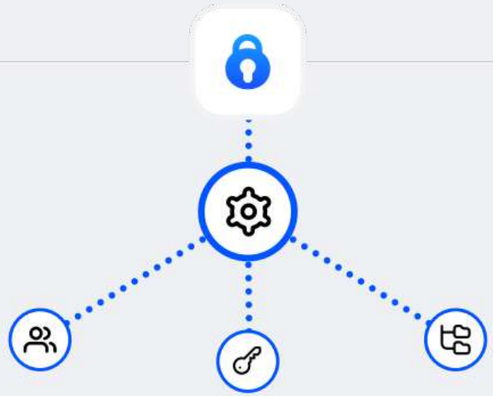
The password manager automatically fills in login form fields, eliminating the need to type passwords using the keyboard. This reduces the risk of password interception by a keylogger.

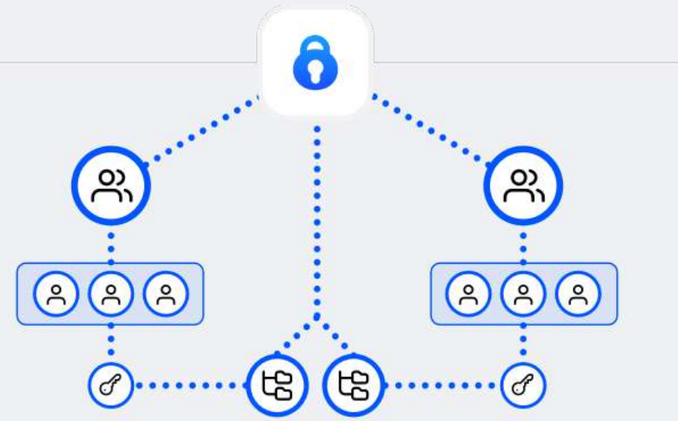
Data encryption

Data is stored in an encrypted form, both locally and in the cloud. Encryption prevents access to private information, including passwords, in a human-readable format.

Secure data sharing between employees

A password manager can significantly assist in the secure sharing of data between employees by introducing several key features and practices:





Sharing directly from the password manager

The password manager allows for the direct sharing of access data within the app, eliminating the need to send it through unsecured communication channels. Employees can share access to confidential information with one another without the need for any transmission.

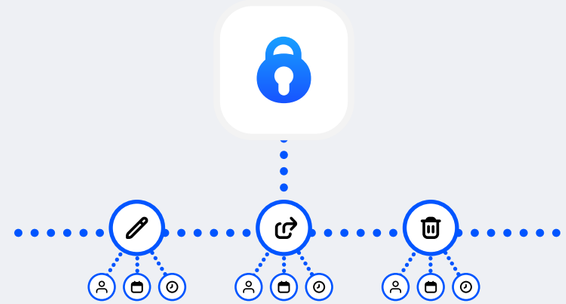
Permission management

The password manager allows for precise management of access permissions. Administrators can specify who has access to which resources and under what conditions, enhancing control over information sharing.

Secure data sharing between employees

A password manager can significantly enhance secure data sharing between employees by introducing several key features and practices:





Secure password sharing with external partners

When collaborating with external partners or suppliers, the password manager enables encrypted sharing of access data, eliminating the need to send it through insecure methods such as text messages.

History and activity tracking

The password manager offers activity tracking and sharing history features. This allows monitoring who had access to specific data and when, which can be useful for security audits.

What makes the Inlockly™ app secure?



The security of your company is our priority.

The approach we use every day is "privacy by design." This means that every design decision begins with a focus on user security, privacy, and the protection of their data.

The information and data stored in Inlockly™ are encrypted, and only you possess the key (on your device) to decrypt them. Inlockly™ is designed to protect users from breaches and other threats. Even developers and other Inlockly™ staff do not have the ability to view or share the user's protected data and confidential information.

Only you can access your data stored in Inlockly™.

Your data in Inlockly™ is fully encrypted to ensure security. We use advanced encryption techniques and security measures such as AES-256-GCM and Argon2id to ensure that only you have access to your information.

GDPR
COMPLIANT

CCPA
COMPLIANT

With your data security in mind

Your master password

It protects your data on the logged-in device. Only you know your master password. It is never sent to the Inlockly™ server.

Your encryption keys

They are created locally on your device and secured with the master password. Encryption keys protect the data in the cloud.

Automatic clipboard clearing

Inlockly™ automatically clears the clipboard after sensitive data, such as usernames and passwords, have been copied.

SafetyMeter™ – your private security guard

SafetyMeter™ is a built-in tool that locally scans your data to detect threats and security breaches.

Automatic device locking

After a period of inactivity, Inlockly™ automatically clears the memory and prompts you to re-authenticate.

We have released a security report.

We have fully documented our project and security mechanisms, providing a detailed description of how the key features of the app work. Anyone can review it on our website at www.inlockly.com.

inlockly

Try it for free for 14 days

The Inlockly™ app on your device:

GDPR COMPLIANT

CCPA COMPLIANT

Your discount code:

EBOOK10

10% discount on your first transaction

Visit us at www.inlockly.com