Due to the rise in data breach incidents in the last few years, businesses have grown increased privacy concerns over [securing customer data](http://www.cardzgroup.com/BankCards.html). With advancement in technology, there is a bigger need to protect information. Thus, individuals and businesses now look for newer methods of securing their data.

From shielding identity to protecting passwords, let’s dive into seven innovative ideas that strive to protect data privacy while making it simpler and accessible.

1. **A Bank Card with Hourly-Changing CVV**

A French company in 2019 specializing in digital payment security introduced a card with CVV that changes every hour. Oberthur technologies introduced this concept on the idea that even if your credit card number is stolen, it cannot be used for transactions for more than one hour. Once the CVV code changes, anyone with the card number but not the CVV cannot do any transaction.

This dynamic CVV technology is known as motion code. It was originally created by a technology company [Idemia](https://www.idemia.com/) in 2016. Rather than the CVV being printed on the back of the card, it is displayed on a tiny screen powered by lithium battery. It refreshes automatically to a different code every hour.

1. **Software Program with Cryptographic Key**

With so many accounts to handle, maintaining different passwords for each account has become a hassle. Keeping the same password for all accounts is also a security risk. Compromised passwords are one of the biggest reasons for data breaches today.

To overcome this, a company called [Nevo](https://dataprivacymanager.net/5-innovative-ways-to-protect-your-personal-data/nevo.id) has come up with an idea to reduce breach incidents by mitigating all vulnerabilities resulting from digital credentials. They achieved this by replacing passwords with cryptographic keys, biometric layers and verifiable digital credentials.

1. **One App for Managing all Privacy Data**

An application named [Jumbo](https://play.google.com/store/apps/details?id=com.jumboprivacy&hl=en&gl=US) allows users to manage all privacy data from one single location. It can change your Facebook privacy, create backup, delete old tweets or even clear Google searches. It was named on the concept that big technology giants don’t forget anything about you. Jumbo, on the other hand, is an elephant that never remembers anything.

1. **Smart System for Encrypting Hardware Devices**

[Winston](https://www.springwise.com/technology-innovation-data-encryption-winston-privacy/) provides smart hardware encryption for all home devices. It’s easy to install and promises the protection of online privacy of its users. It has a hardware filter that safeguards home connected devices. The best thing is that it works with streaming services, devices and websites. Its algorithm is based on breaking and encrypting a user’s internet activity and location along with some other Winston users.

1. **Decentralized and Open-Source Search Engine**

An open-source search engine by the name of [Presearch](https://www.springwise.com/a-decentralised-search-engine-with-crypto-rewards/) comes with increased privacy settings. It’s a decentralized engine built on blockchain, and pays users in the form of cryptocurrency tokens. The search engine hopes that it can break Google’s dominance in the search engine market.

Users can buy keywords sponsorship through cryptocurrency but cannot be tracked for what they search over the internet. Thus, they aren’t bombarded with targeted ads related to the search history.

1. **Fingerprint Authentication for Approving Card Transactions**

[A bank card by NatWest](https://www.springwise.com/uk-bank-pilots-fingerprint-sensitive-bank-cards-for-contactless-payments/) requires a user’s fingerprints instead of PIN code. Users first need to register their fingerprints at the bank. However, the fingerprints are stored on the card and not at the bank’s database. However, the digital security company Gemalto that designed the card says that the card still works with contactless technology or a PIN code.

1. **Messaging Platform Shielding User Identity**

[Signal](https://signal.org/en/) is a messaging application with end-to-end encryption to protect its user’s privacy. Its sealed sender feature offers increased security by encrypting information related to the users messaging each other on the platform.

These are few examples of how you can increase data security and privacy and be innovative simultaneously. Both technology and innovation are imperative to build a future that provides technological growth along with ensuring security.