With the upsurge in data breach incidents over the past years, privacy concerns for businesses have continued to rise. As technology is advancing, so is the need for information protection. Businesses and individuals are now discovering new data security methods.

Ranging from identity shielding, end-to-end encryption and password protection, let’s look at five innovative ideas that aim to make data protection more accessible and simpler.

1. **Bank Card with CVV that Changes Every Hour**

In 2019, a French digital payment security company known as Oberthur Technologies introduced a new card with dynamic CVV that changes every hour. If criminals get hold of your [credit card](cardzgroup.com%20or%20http:/www.cardzgroup.com/ContactSmartCard.html), they cannot use it for more than one hour. Once the security code changes, the card is rendered useless for anyone who has the card number but not the changed CVV.

The technology behind the dynamic CVV is known as motion code. Originally, it was developed by a tech company named Idemia in 2016. Instead of the CVV printed at the card’s back, the motion code CVV is displayed on a mini screen, and automatically refreshes to a random code every hour. The screen is powered by lithium battery. Other than this, the rest of the card looks like just any other card.

1. **Software that Replaces Your Password with Cryptographic Key**

As passwords increasingly become the target of phishing attacks, maintaining them has become a difficult task. Data breaches mostly result due to human error, and not because of malware, as commonly assumed. According to a [report](https://www.shredit.com/en-us/about/press-room/press-releases/sacking-employees-for-data-breach-negligence) by a security company called ShredIt, about 47 percent of C-Suite Executives and Small Business Owners said that employee negligence had resulted in data breach at their organization. Around one-third of the breaches were related to compromised passwords.

A Los Angeles based company called [Woven](nevo.id) (now Nevo) was created with the idea of reducing risk of security breaches to enterprises by mitigating the vulnerabilities related to digital credentials. They implemented this by replacing a user’s password with cryptographic key, multiple biometric layers and digital credentials that can be verified. The credentials are not related to companies but the individuals themselves, so you can carry them from one employer to another.

1. **An App that Manages all Your Privacy Data**

[Jumbo](http://www.jumboprivacy.com) is an app that promises users to manage all their privacy settings from a single location. With just one tap, it can change your Facebook privacy settings, create backups and even delete old tweets, Alexa voice queries or Google searches.

The name Jumbo was given to the app based on the concept that tech giants never forget what you post or type in search bar. Jumbo, on the other hand, is a big elephant that never remembers anything. The app doesn’t communicate with any server and all user communication takes place on the user’s phone. This means that Jumbo does not even know or remember who is using the app.

1. **Smart System the Encrypts Hardware Devices**

[Winston](https://winstonprivacy.com/) is a smart hardware encryption system for all your connected home devices. This easy-to-install system promises to protect a user’s online privacy. When running, its hardware filter protects all connected devices at home.

It works with all devices, streaming services and websites, including webcams, WiFi routers, Smart TVs and even Amazon’s Alexa. The algorithm works by breaking and encrypting the location and internet activity of a user with that of a group of twenty or thirty other users of Winston. This group keeps changing every hour, thus making it impossible to follow or track a particular individual or home.

1. **An Open-source, Decentralized Search Engine with Increased Privacy**

[Presearch](presearch.org) is a decentralized, opensource search engine that comes with improved privacy settings. The search engine is built on the blockchain, and also pays its users in cryptocurrency tokens. It hopes to break the dominance of Google in the internet search engine market.

You can use cryptocurrency to buy keyword sponsorship for your advertisements, but users are not tracked for their searches. This means that they are not targeted any ads related to their search history.

These ideas are an example of how it’s possible to enhance data privacy while being innovative at the same time. Both go hand in hand and are essential to build a future that promises technological growth and protection.