Michael Woodmansee

Smart Card

Over the past few years , we have heard of Facebook or currently use it.

Throughout this Smart Card we will go through what to do and don't do ,privacy features, how companies have access to your data on facebook and other useful features.



**Good Things to Do**

1. Review your settings page sidebar.
2. Setting up Two-Factor Authentication
3. View the “My Facebook Information” option in the settings.

**Good Things Not to Do**

1. Not setting up Two-Factor Authentication
2. Never reviewing your settings page
3. Giving access to your data to unknown sites or companies.

**Privacy**

This is where manganing profile is up to the user and how much they other people of the users profile.

If the user ignores the settings and just starts using the site, then when other users will see most but not all.

The user can set who see what like what friends see while this feature is limited in the setting on the main page, any post or shared link, photos or other media can be set to who can view it.

**Accessibility**

When it comes to control over your Facebook account. Facebook lets their users delete or deactivate their account.

Any app the user access with their Facebook account will have access to Facebook data along as the user uses the app.

**Encryption / 3rd Party Data**

Do third parties have access to your Facebook data? Yes and No.

While Facebook stated that they don’t sell the data , they do use basic information like age, gender, and interests to target ads to specific people.

Because Facebook uses targeted ads they are not selling user data but sharing the demographic info of their user base.

On the side of data encryption , Facebook doesn't use end to end encryption, but uses an encryption to scramble the messages. This type of encryption is pretty common in the industry.

**Other useful information**

1. That most of user base doesn't read the terms of service, or the privacy documents (Pretty common)
2. Most privacy conscens can just be avoided by not involving yourself in them. (Look up “Risk avoidance”)