bitwarden | Help Center Article

SECURITY

# Vault Data

View in the help center:
https://bitwarden.com/help/vault-data/

## Vault Data

All vault data is encrypted by Bitwarden before being stored anywhere. To learn how, refer to the Bitwarden Security Whitepaper. Bitwarden is a zero knowledge encryption solution, meaning you are the only party with access to the keys required to decrypt the vault data.

Listed below are examples of the data that is encrypted, as well as download links demonstrating the encrypted data.

> **Tip**
> We encourage you to review our privacy policy for more information.

Vault data that is encrypted:

- For all items:
  - Item names
  - Notes
  - Attachments
    - Attachment name
    - File contents
    - File encryption key
  - Custom field names and values
- For logins:
  - Usernames
  - Passwords
    - Password history
  - URIs (i.e. match detection strings)
  - Authenticator keys (i.e. TOTP secrets)
- For cards:
  - Cardholder names
  - Numbers
  - Brands
  - Expiration dates

  - Security codes
- For identities:
  - Names (Title/First/Middle/Last)
  - Usernames
  - Companies
  - Social Security numbers, passport numbers, and license numbers
  - Emails and phones
  - Address 1, Address 2, Address 3, City / Town, State / Province, Zip / Postal code, Country
- For Sends:
  - Send names
  - Send text
  - Send file
  - Send notes
  - Send encryption key (learn more)
- Folder names
- Collection names

Secrets Manager data that is encrypted:

- For secrets:
  - Secret names
  - Secret values
  - Secret notes
- Project names
- Service account names
- Access token names (access token values are never stored by Bitwarden)

Some data, but **never vault or secrets data,** is used to provide the Bitwarden service to you. This is referred to as administrative data and can be accessed by Bitwarden. Learn more.