



openHPI Course: Digital Identities – Who am I on the Internet?

# Password Manager

**Prof. Dr. Christoph Meinel**

Hasso Plattner Institute  
University of Potsdam, Germany

# Password Manager

---

## Problem of secure passwords

- Each password-based account/identity has its own password
- Many user have >20 internet accounts/identities
  - **Can't remember all passwords**

## One possible solution: **Password Manager/Safe**

- Service or program, that manages/encrypts all passwords with a single strong password
- Helps generate “complex” passwords and warns of insecure weak ones
- Automatic entering password on websites/services
- Exists as offline and online variants
- Already integrated in a number of browser

# Offline Password Manager

---

Data is stored locally on the user's device in encrypted form

- **Advantage:** No third party has access to passwords

- **Disadvantage:**

  - data is only local to user's device

    - Synchronization needed

  - hardware defect or theft endangers passwords

    - Backups needed

- Open-Source (i.e. KeePass) and commercial solutions available (i.e. 1Password)

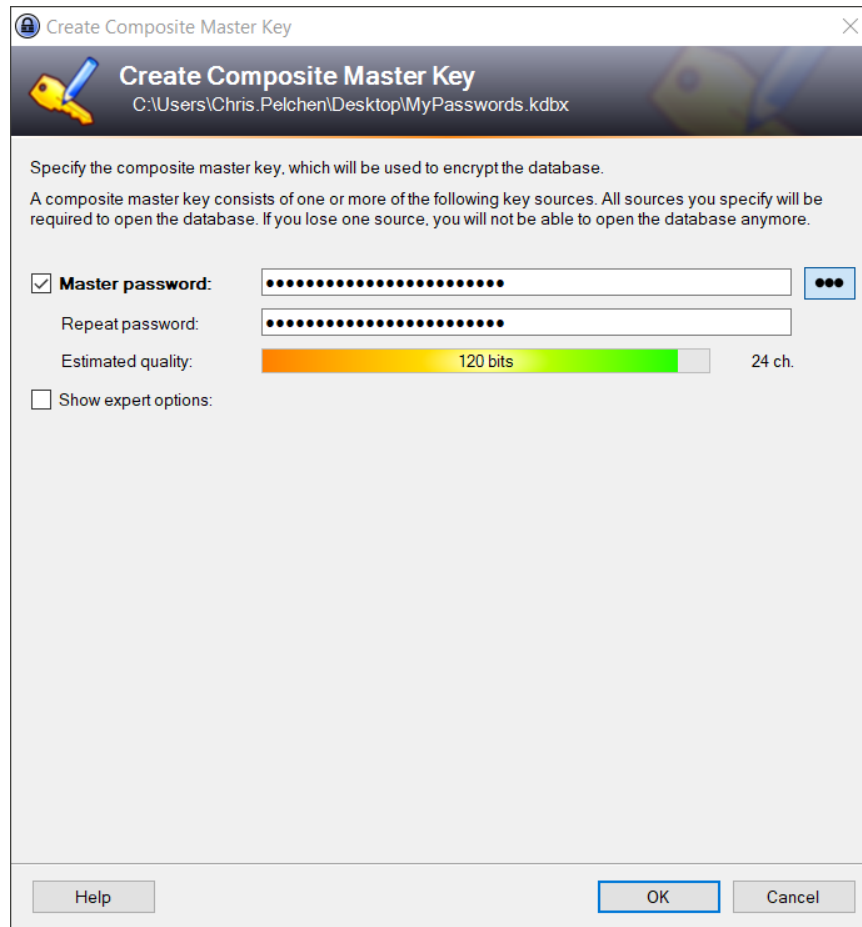


**KeePass**

**1Password**

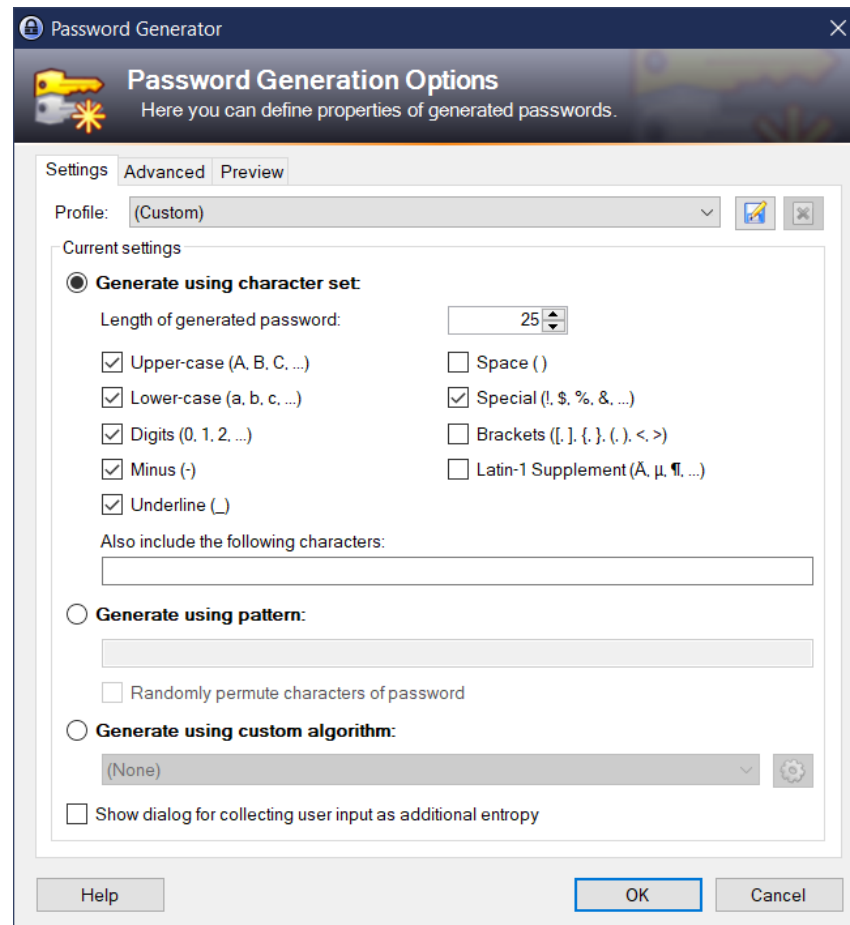
# Example – KeePass (1/3)

- Set master password when creating a new database



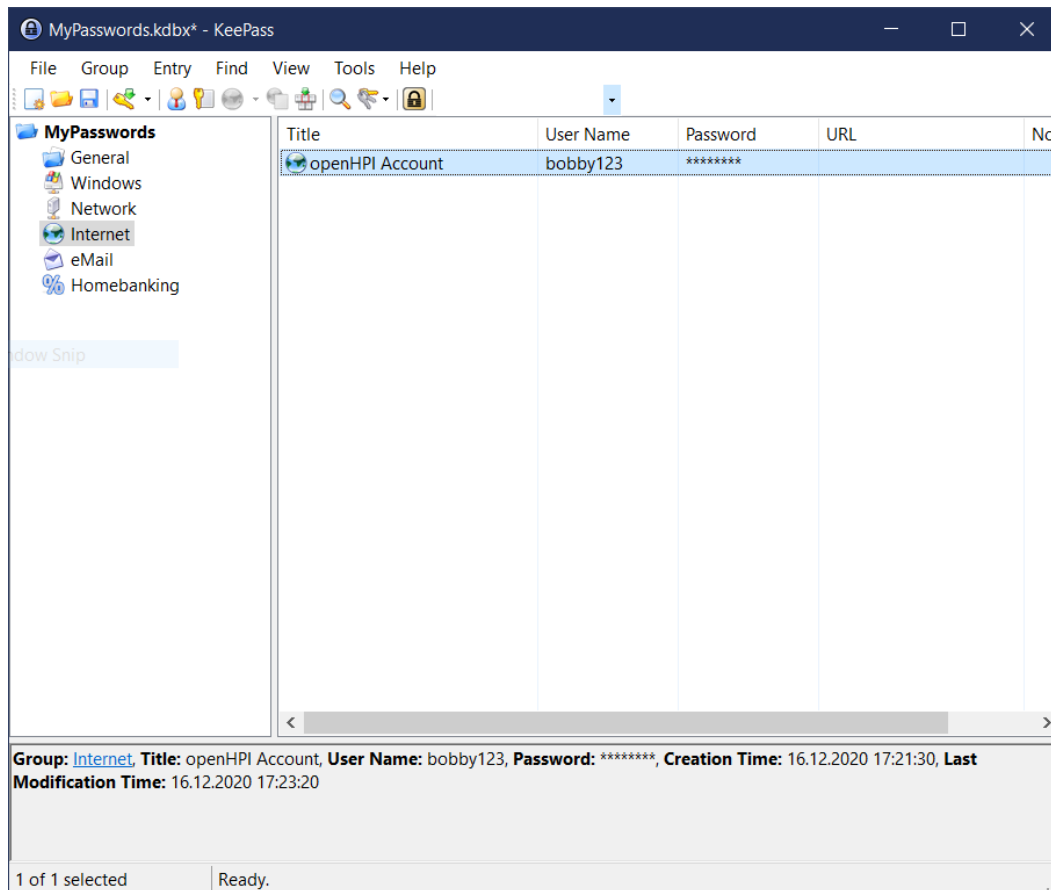
# Example – KeePass (2/3)

- Generate strong passwords for each new account



# Example – KeePass (3/3)

- Easy access to all credentials in the database



# Online Password Manager

---

Password manager is offered as an online service

## ■ **Advantage:**

- passwords are synchronized and available on all devices
- theft of single device or hardware defect is not a problem anymore

## ■ **Disadvantage:**

- dependent on provider
  - **availability**
  - **confidentiality** – How do providers store passwords?
- Often commercial providers (i.e. LastPass, Dashlane)

# Password Manager Within Browsers

---

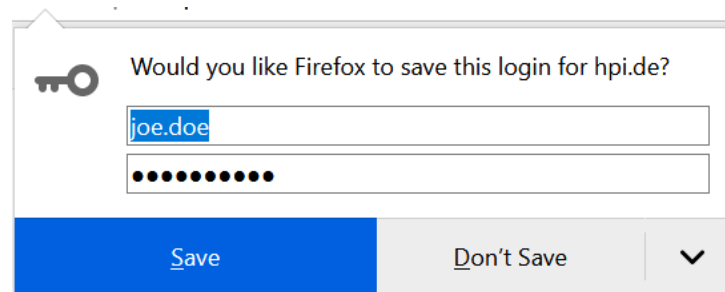
- All popular browser vendors (Firefox, Chrome, Safari) offer password managing in the browser
  - sometimes even a check with a password leak databases is possible
- Typically they are offline password managers
  - synchronization possible via Sync (Firefox), Google Account (Chrome), iCloud Keyring (Safari)
- **Beware:**
  - master passwords for protecting your password **deactivated by default**
  - access to passwords easy when browser accessible



# Password Manager Within Browsers

- All popular browser vendors (Firefox, Chrome, Safari) offer password managing in the browser

🔑 Use a Securely Generated Password  
yyLCqpwV2QnE6Bf  
*Firefox will save this password for this website.*



Would you like Firefox to save this login for hpi.de?

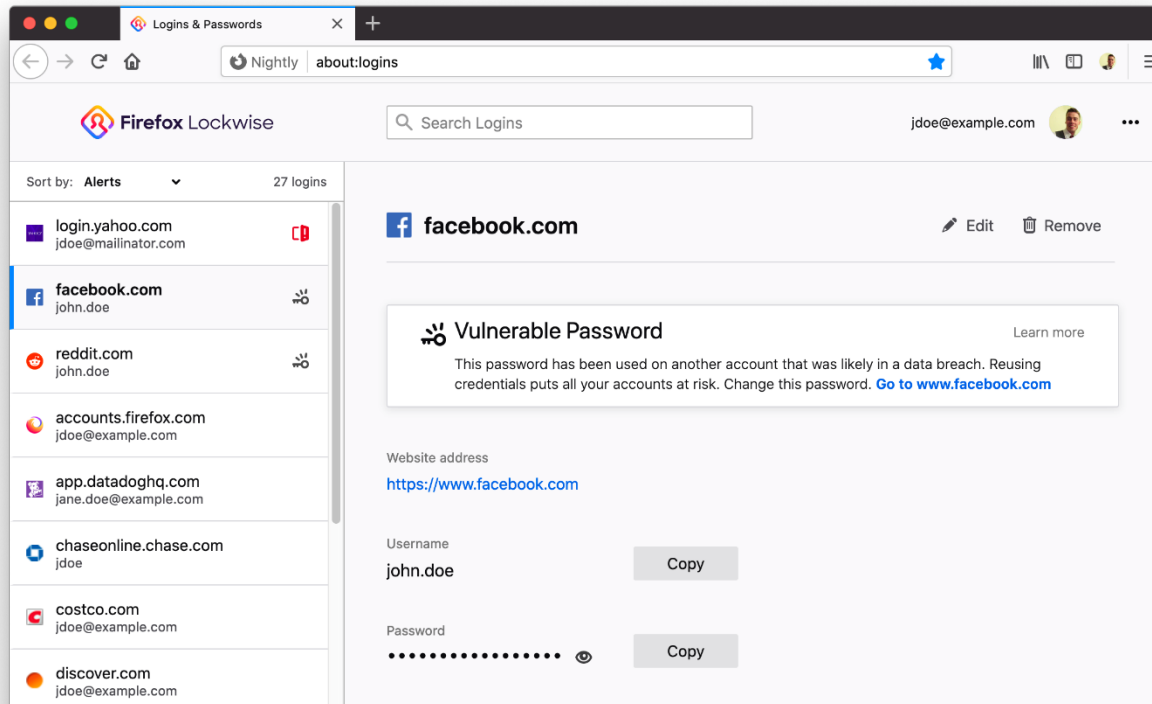
Username: joe.doe

Password: ••••••••

Save Don't Save ▼



# Password Manager Within Browsers



Check with a password leak databases is possible

## Password Checkup

Your passwords were exposed in a third-party data breach. You should change them now.



[Go to Password Checkup](#)

# Password Manager in Browsers

---

- Typically they are offline password managers
  - Synchronisation possible via Sync (Firefox), Google Account (Chrome), iCloud Keyring (Safari)
- **Beware:**
  - Master passwords for protecting your password **deactivated by default**
  - Access to passwords easy when browser accessible

# Discussion

---

## Password managers offer multiple advantages

- Complex passwords can be automatically generated
- Integration in browsers to ease work processes, e.g.
  - automatic input in login forms
- Access can be secured with other (multi) factors possible

## Usage needs to be thought through

- Master password needs to be secure
- Access by unauthorized people dangerous, especially without master password
- **Availability** vs. **confidentiality** has to be weight against each other for decision **online** vs. **offline**