OKTHANKS
OKTHANKS.COM

OKTHANKS USER INSIGHTS

into

KEEPASSXC

MARCH 2019

> *It gives you peace of mind knowing you will never forget a password again and you can recall those passwords at anytime.*

— Participant A

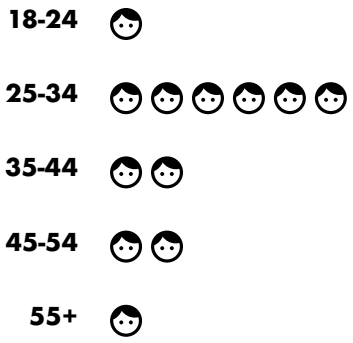
INTRODUCTION

The need for and access to digital security and privacy tools that protect our user data is growing! However, many of the tools available struggle with being inclusive. The U.S. government created standard measurable guidelines for accessibility which include four principles; operable, understandable, perceivable, and robust. In order to answer the question, “What is the single barrier to use for KeePassXC?” we deployed a study to understand the accessibility, inclusivity, and understandability of KeePassXC. The goal of this study is to answer, “Can anyone use it?” The responses varied. Some people knew how to set it up while others were very overwhelmed and couldn’t complete the setup process. After the setup process was complete, no one was clear what to do next. Although all participants understood the objective of KeePassXC, no one knew how it would function in their daily routine. The following insights seek to answer the question and define barriers to use for KeePassXC.

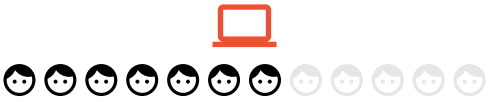
“After the setup process was complete, no one was clear what to do next.”

Demographics

To form a comprehensive view of ‘anyone’ in the search to answer, “Can anyone use it?”, we engaged 12 participants with a variety of ages, education levels, and self identified tech savviness.



Most (10/12) of our participants were between 25-54 years of age. Ten out of 12 participants held an undergraduate degree or above, and 7 out of 12 participants rated themselves as being tech savvy.



OBJECTIVE 1:

HOW WELL CAN PEOPLE EXPLAIN KEEPASSXC TO SOMEONE?

Activity 1 - Explain It

To begin, we printed out the KeePassXC home screen and asked participants to familiarize themselves with it. We then asked them to explain it: first to a friend and then to a grandparent. These two activities lent insights into ways people communicate and explain technical software. We hoped to gain insights regarding language which might be more approachable or friendly. Out of the two activities, we found that when participants were asked to explain it to a friend, their explanation's contained similar language and jargon used within the KeePassXC home screen. However, when asked to explain it to a grandparent, many participants answers were much shorter, contained less technical words and used friendly tones and examples.

100%

of participants, explained it to a friend in a way that fits within the objectives of KeePassXC

100%

of participants, explained it to a grandparent that fit within the objectives of KeePassXC

SOME WAYS PARTICIPANTS DESCRIBED KEEPASSXC:

"It's like a digital wallet to keep all your passwords"

"A safe place so you don't have to go search around, nor do you have to worry about forgetting where they are"

"Keeps track of all your passwords"

"Is a way for you to save all your computer passwords, without having to retype them or remember them, and it's great because you can use it in all your systems you might use like, your iPhone, iPad, and computer, for all the websites you like to look at"

Activity 3 - Unfamiliar Words

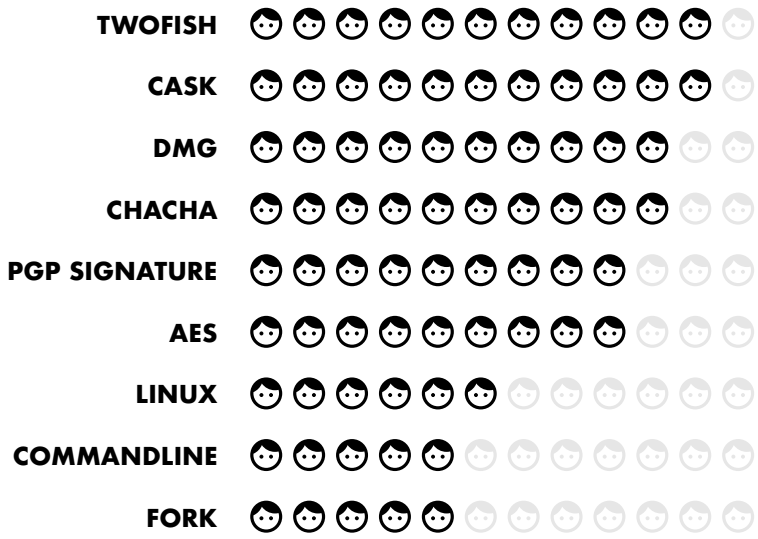
To assist in determining barriers to using KeePassXC, we deployed an activity where participants circled words that were unfamiliar to them in the download and setup process.

WORDS USED IN ACTIVITY

password manager **Windows** **autofill** **Cask**
notebook **fork** **master key** **memo** **bundle**
Homebrew **entry** **sourcecode** **main password**
browse **Commandline** **storage** **Installer** **key**
key file **challenge response** **Twofish** **interface**
password **keeper** **auto-type** **database** **encryption**
PGP signature **url** **repeat password** **ChaCha** **beta**
refresh **verify** **macOS** **open source** **root** **Linux**
file **DMG** **CSV import** **re-type** **passphrase**
AES **binary** **integration** **cross platform**

Some words were added for testing purposes.

UNFAMILIAR WORDS



In the same activity, we had participants underline any words that have a negative association with the participant. 7 out of 12 participants did not underline any words.

RECOMMENDATIONS FROM OBJECTIVE 1

KeePassXC does a good job of explaining what a password manager does, but some words used on the home page are too technical or confusing for the 'anyone' user. Thus, creating a barrier to use through language. We recommend making some minor changes to the language used on the homepage and download page, updating it to be more approachable or friendly to the 'anyone' user.

FAMILIARIZE LANGUAGE ON HOME AND DOWNLOAD PAGES

STATE CLEARLY HOW THE APP WORKS IN DAILY LIFE ACROSS ALL DEVICES

STATE CLEARLY THE BENEFITS OF THE APP OVER OTHER OPTIONS

> ***I thought it was very self explanatory and made sense. However, the homescreen jargon needs to be more friendly, approachable and relatable for the younger generation otherwise they will ask, "What does this mean?" "Why care?"***
>
> **— Participant L**

OBJECTIVE 2:

WHERE ARE BARRIERS IN THE SETUP PROCESS?

Activity 2 - Setup KeePassXC

The second portion of the study was to have participants setup KeePassXC, create a new database and enter passwords. This was a self-led activity seeking to capture, “Can anyone set it up?” It was also a search for any confusion points along the setup process. To be grounded in the reality of people’s busy lives, we first asked, “In a typical day, how much time would you spend setting up a password manager?” The average time people allotted was 25 minutes. Participants then set a timer for their chosen time and began the setup process.

AVERAGE TIME ALLOTTED FOR SETUP – 25MIN

“Can anyone set it up?”

How Far People Made it Through Setup

Fifty percent of participants made entries into the root dashboard view and considered setup complete. However, the other 50% of participants either entered a master key and stopped, or made it to the root dashboard screen without entering any passwords. Overall, participants seemed to understand what KeePassXC is, but were confused within the UI. They were not always clear what to do next, nor confident when they had completed setup. People who are familiar with or already use a password manager understood overall how to setup KeePassXC, but when we asked how they expected KeePassXC to work in everyday life, 100% were unclear. To help determine confusion or pain points along the setup process, participants created lists of when they were stuck or confused. These points may be helpful in deciding where the barriers for use lie.

SPLIT 50/50

Confusion Points

The following paraphrased comments capture participants confusion points along the setup process for KeePassXC.

- ***After creating a database, I went to the top left to add a password, but it was the button to create a new database. I would expect that once the database is created, it would go into the background. It should be more obvious that I'm in the database and working there instead of being able to create more databases in a string.***

- ***I clicked 'create new database,' but I wasn't sure if that was what I was supposed to do because there were other options like 'import,' 'open existing,' etc.***

- ***I'm unsure where I should start entering the passwords.***

- ***I'm in the 'root.' Now what?***

- ***I think I've added all passwords. Not sure what to do now.***

- ***I tried to copy and paste, but paste wouldn't work and I got an error.***

- ***There's no clear action or leading step (prompt) to guide me to 'begin entering passwords' or 'start'.***

- ***When it asks to save a file, I'm not sure what this file is or why I'm saving it.***

- ***What does 'perform auto-type' do?***

- ***How do I know I saved the right password for use?***

- ***It didn't tell me my master password was insecure. For such a secure password manager it accepted a very insecure master password.***

- ***The root screen didn't look correct for setting up passwords.***

- ***I was confused about encryption settings (see below).***

Many participants found this screen confusing.

What People Expected to Happen Next

Four people ended setup on the root dashboard view and did nothing more. Six participants who made it to the dashboard view thought the setup was complete for the purpose of the activity. Out of the 12 participants, 6 made entries into the root dashboard view and considered setup complete. We then asked how they expected it to behave. Answers varied.

The following paraphrased comments capture what participants expected to happen next in the setup process.

- ***When I go to a website, I would expect it to ask me if I want to enter my saved password. Then it would fill it in for me.***
- ***I expect to be able to access it from all of my devices. I would have to be able to do that or I wouldn't use it.***
- ***I would expect it to work like Apple keychain.***
- ***I think it would tell me I'm finished with this part of setup, then tell me what to do next.***
- ***I'm not sure.***
- ***I have no idea.***

RECOMMENDATIONS FROM OBJECTIVE 2

The results of this section were split 50/50. However, to create an application that 'anyone can use,' will require a few recommended updates. It was clear that encryption settings were confusing for all participants no matter their level of familiarity or tech savviness. In the root view, it was unfamiliar and unclear to some to enter passwords, let alone *how* to begin entering one. Participants wanted to be prompted on what to do next. They were also unsure when the setup process was complete and expected a 'save' or 'finished' button. They were unclear about how to access their information after they entered it in. Since participants are unclear how to use KeePassXC in their daily life, we recommend a prompt to install the web plugin and be clear that all entries are saved and stored for later access.

REVAMP ONBOARDING WORKFLOW SO PASSWORDS ARE ACCESSIBLE FROM ANY DEVICE

MAKE FINAL STEP CLEAR AND PROVIDE MORE CONFIRMATION THROUGHOUT THE SETUP PROCESS

MAKE ENCRYPTION SETTINGS MORE ACCESSIBLE OR REMOVE THEM AS A REQUIRED STEP IN SETUP

CONCLUSION

From our study with 12 participants, it was clear there are some barriers to using KeePassXC. We learned that although people have a general understanding of what KeePassXC is, 100% of them are confused about how to actually use it in life and only 50% of them were able to complete the setup process. The actual barriers varied from unknown language and confusing UI to unclear process steps for setup and a foundational understanding of how KeePassXC actually functions in one's workflow, therefore making adoption difficult. We suggest the following recommendations, based on insights learned. If KeePassXC is really interested in making KeePassXC approachable and easy to use by 'anyone' our number one recommendation is to revamp the onboarding process.

OVERALL RECOMMENDATIONS

Break Down the Barriers

CREATE A COMPREHENSIVE ONBOARD WORKFLOW

- **FAMILIARIZE LANGUAGE ON HOME AND DOWNLOAD PAGES**
- **STATE CLEARLY HOW THE APP WORKS IN DAILY LIFE ACROSS ALL DEVICES**
- **STATE CLEARLY THE BENEFITS OF THE APP OVER OTHER OPTIONS**
- **MAKE FINAL STEP CLEAR AND PROVIDE MORE CONFIRMATION THROUGHOUT THE SETUP PROCESS**
- **MAKE ENCRYPTION SETTINGS MORE ACCESSIBLE OR REMOVE THEM AS A REQUIRED STEP IN SETUP**
- **CONSIDER MODERN UI SKIN**
- **ADDRESS UI CONCERNS IN DASHBOARD VIEW**

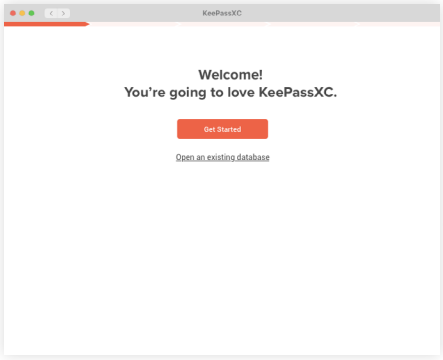
NEXT STEPS

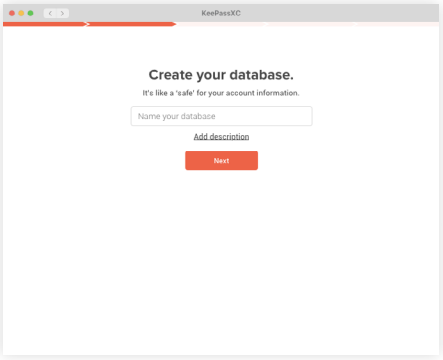
DETAILED RECOMMENDATIONS

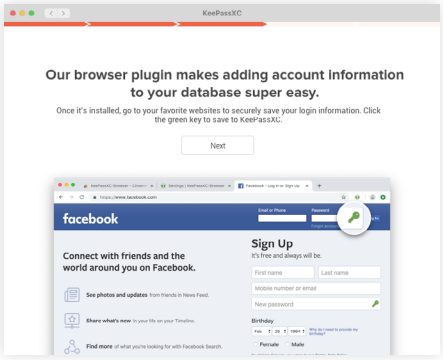
1—Create a Comprehensive Onboard Workflow

A comprehensive onboard workflow brings the user from downloading the app to having it ready for everyday use. The outcome of a first-use experience should be a filled database that is connected to the user's preferred browser.

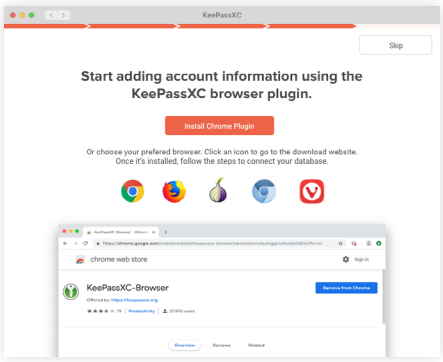
The wireframes that follow outline a workflow that brings users through a complete first-use experience. Access the interactive design prototype here. *Note: This experience is dependent on the browser plugin meeting expectations outlined in the next section.*

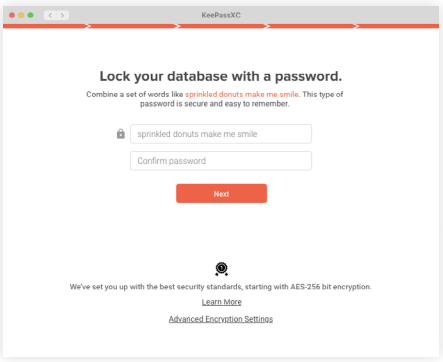


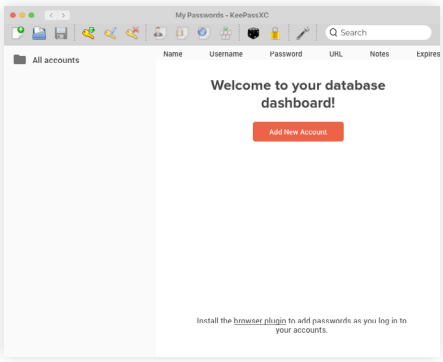


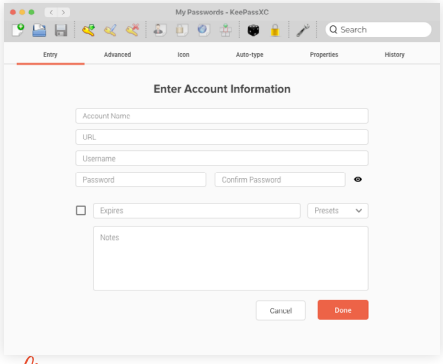


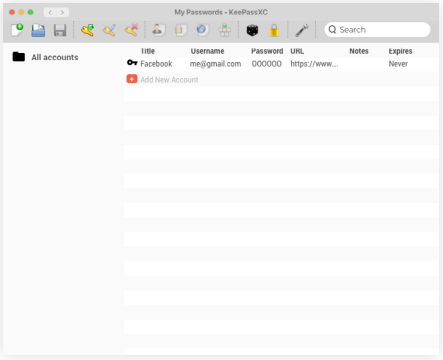
Full page views start on page 16











THE OUTCOME OF A FIRST-USE EXPERIENCE SHOULD BE A FILLED DATABASE THAT IS CONNECTED TO THE USER'S PREFERRED BROWSER.

2—Basic requirements for the Browser Plugin

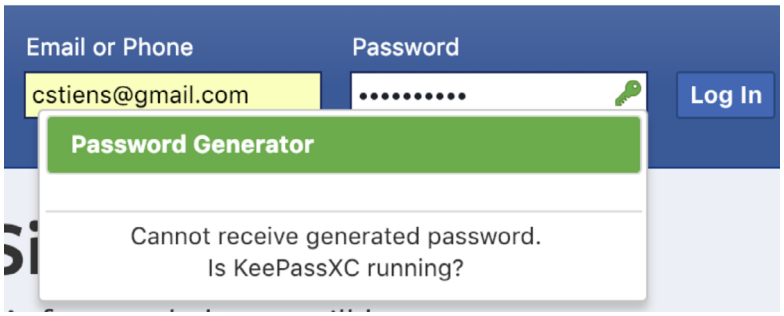
In order to help KeePassXC reach its full capabilities, we've outlined user expectations to guide UX improvements for the browser plugin. At the highest level, the plugin should:

- **WORK AS THE USER EXPECTS**
- **WORK RELIABLY WITHOUT ERRORS**
- **FAIL BEAUTIFULLY IF THERE IS A PROBLEM**

SETTING UP THE BROWSER PLUGIN

The user would expect...

- To be prompted to connect their database by entering their master password if they have an existing database
- To be prompted to finish onboarding if their connected database is incomplete
- To be notified that the plugin is remembering and storing information in their database
- For the plugin to work seamlessly with the desktop app
- For the plugin to make updating passwords in their database seamless



GENERATING NEW PASSWORDS

The user would expect...

- To only be prompted to generate a password if they were on a site and creating an account for the first time
- An offer to generate a password when they create an account or set a password for a site that isn't saved in their database

REMEMBERING PASSWORDS

The user would expect...

- All generated passwords to be saved to their database
- The plugin to offer to remember the password they created manually if they opted out of a generated password
- To be prompted to change passwords that have expired if they didn't set an expiration date in their database
- To be prompted to allow the app to remember their password if they have a database connected, but are accessing an account they haven't saved to it yet

AUTOFILLING PASSWORDS

The user would expect...

- The key icon in the password field to autofill their information if it is saved to their database

3—Familiarize Language

- **CONSIDER A NEW WORD FOR 'DATABASE'**
  From debriefing with participants, we learned that 'database' wasn't an unfamiliar word to them, but it was confusing in this context.
- **CHANGE 'ROOT' TO 'ALL ACCOUNTS'**
  Many people were confused about the root folder and what it meant.
- **SWITCH FROM THE NOTION OF ADDING 'PASSWORDS' TO ADDING 'ACCOUNT INFORMATION'**
  To capture the entirety of KeePassXC's capabilities, we recommend highlighting that the app not only stores the password, but all account information and any other details the user desires.

4—Address UI Concerns in Dashboard View

Based on the previously stated confusion points on page 8, we've highlighted those specifically related to the dashboard view

- ***It was confusing to have 'new database' as the first action in the dashboard. People expect to be in the dashboard environment already. The first action should reflect the action they would likely take next after they've created a database.***

- ***It was not clear what to do next once participants were in the dashboard view for the first time.***

- ***It was not clear where to start entering passwords.***

- ***When you add an entry, it's not clear how to go back.***

5—State clearly the benefits of the app over other options (by positioning it differently)

At its core, KeePassXC addresses the basic security of needing a password manager. People need unique passwords for each account, but remembering them can be difficult. KeePassXC offers a safe place to put them and see them at any time.

Last Pass and 1Password have a strong emphasis on remembering and filling in your passwords on every device, but we recommend that when promoting KeePassXC emphasize what it does really well—stores your passwords securely.

We suspect that there is a niche market of users where the need and desire to store passwords on a local computer rather than in the cloud is of utmost importance. Further research would help define these use cases and provide an understanding of the size of the need and market.

"We recommend that when promoting KeePassXC, emphasize what it does really well – stores your passwords securely."

The objectives of further research would be to discover...

- Users' needs related to protecting accounts
- Users' model for using a password manager
- Which devices they use
- Which devices they commonly log in and out of accounts on
- The importance of having a password manager that works on every device
- Users' threat model for storing sensitive information on local devices

BENEFITS TO HIGHLIGHT

The following features stood out to test participants. The first was also highlighted by a key digital security expert training on KeePassXC in Latin America. Below each function, we've included guiding language for writing content for the homepage.

STORED ON YOUR COMPUTER, NOT THE CLOUD

Your passwords and account information live securely on your computer instead of in the cloud —making it difficult for 3rd parties to intercept.

HAVING CONTROL

Ease your need to remember, but stay in control of your passwords. You can easily find them anytime along with additional account information and notes you may want to add.

PASSWORD GENERATION

Let us generate strong passwords for you. Get serious about protecting yourself. In one day, you can dramatically improve the security of your accounts.

QUESTIONS & CONCERNS THAT WERE RAISED

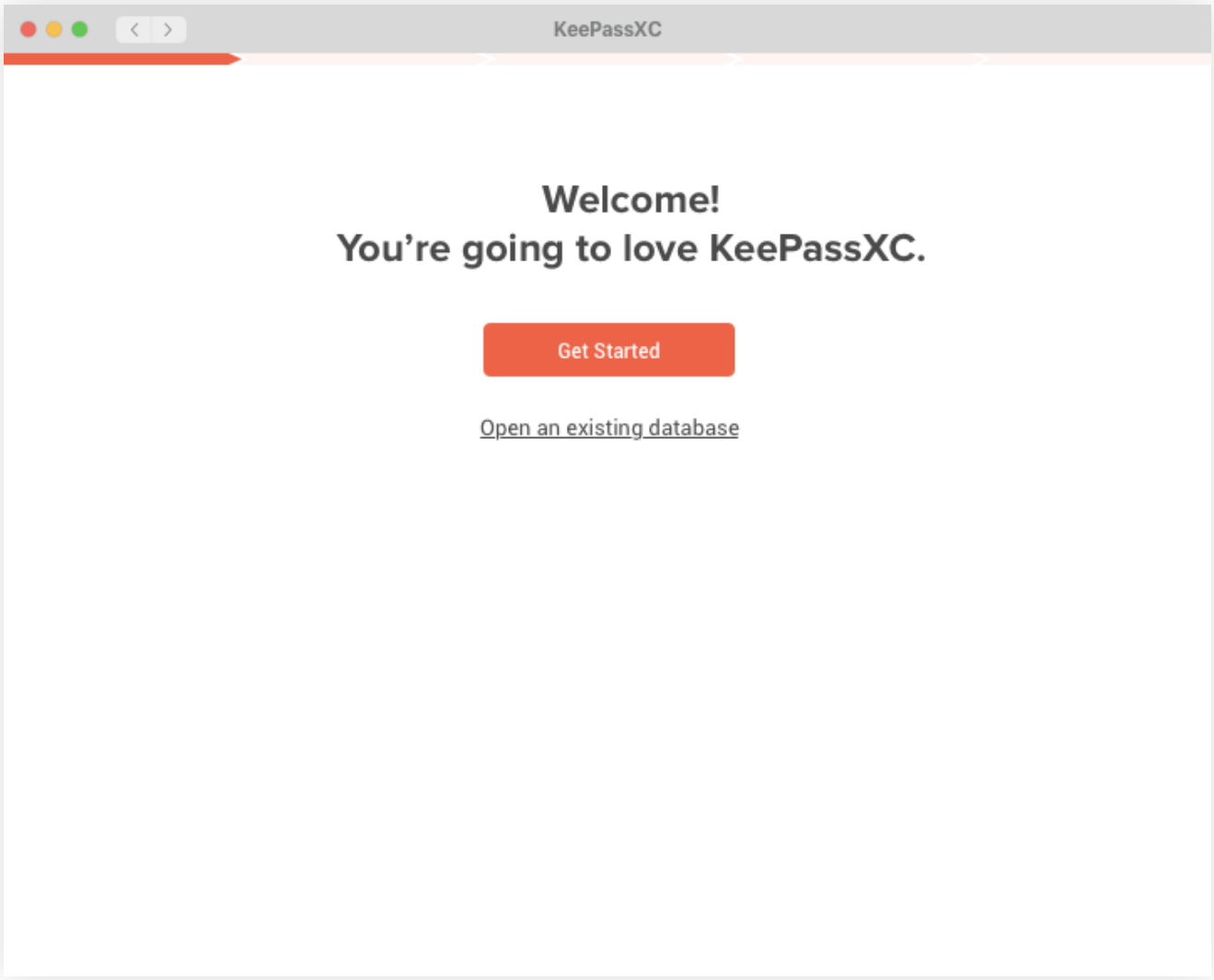
The following list of questions and concerns were expressed in participant debriefs. We recommend amiably addressing these on an FAQ page. Provide tutorials when necessary.

- ***Is it backed up anywhere? What do I need to do to back up my database?***
- ***If I update my database on one device, does it automatically update on my other devices? If not, what do I need to do? What happens if I don't update the database on my phone and I try to login to a website using autofill?***
- ***If I change my password for a site, does it automatically update in my database? If not, what step do I need to take to make sure everything is up to date in my database?***
- ***How do I use the password generator to upgrade my current login passwords to something way more secure?***
- ***How do I get it to sync across multiple devices?***
- ***Can I use it within my team (multiple users accessing the same database)?***
- ***Which passwords should I store here?***

THANK YOU!

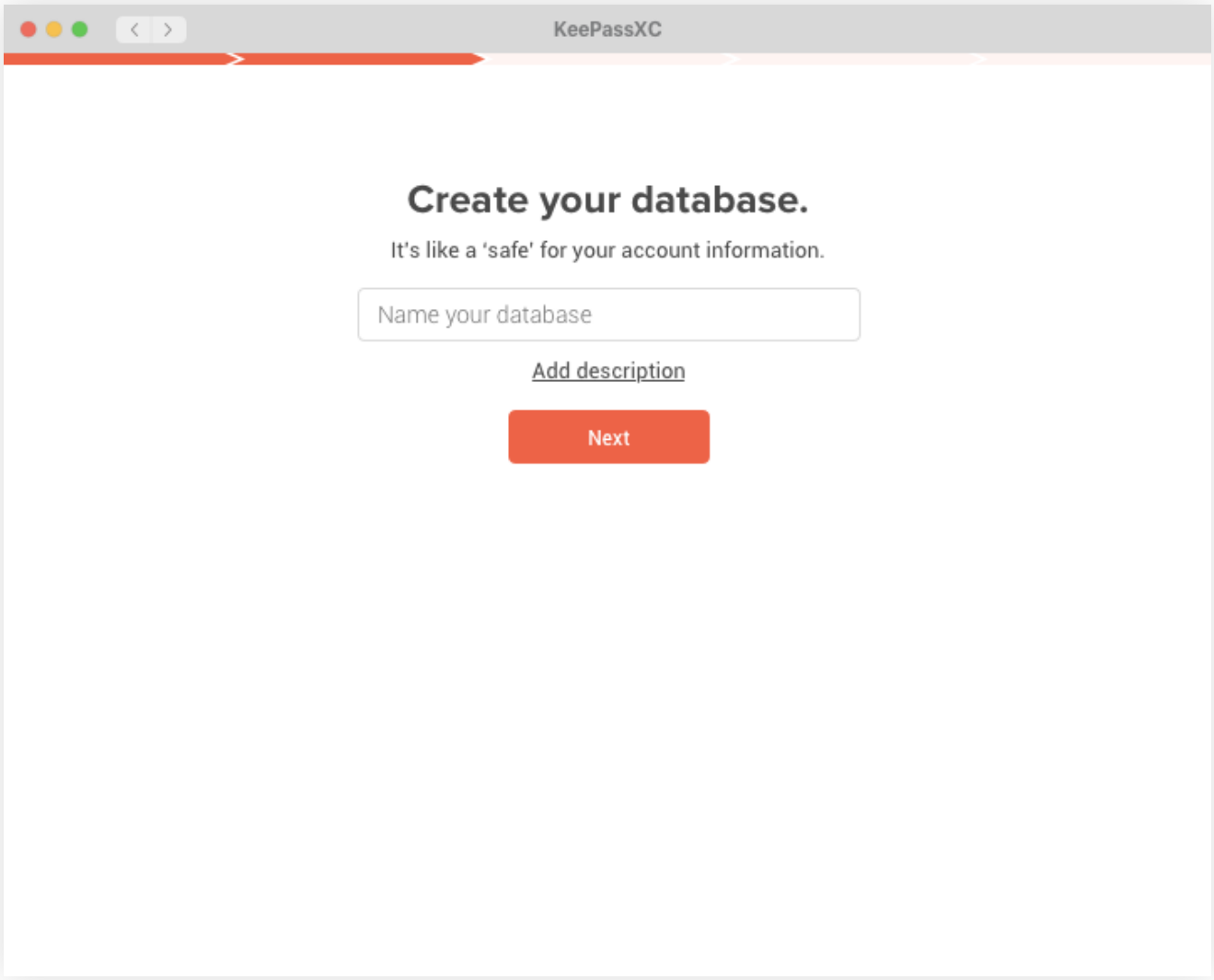
ONBOARD SCREEN 1

Welcome



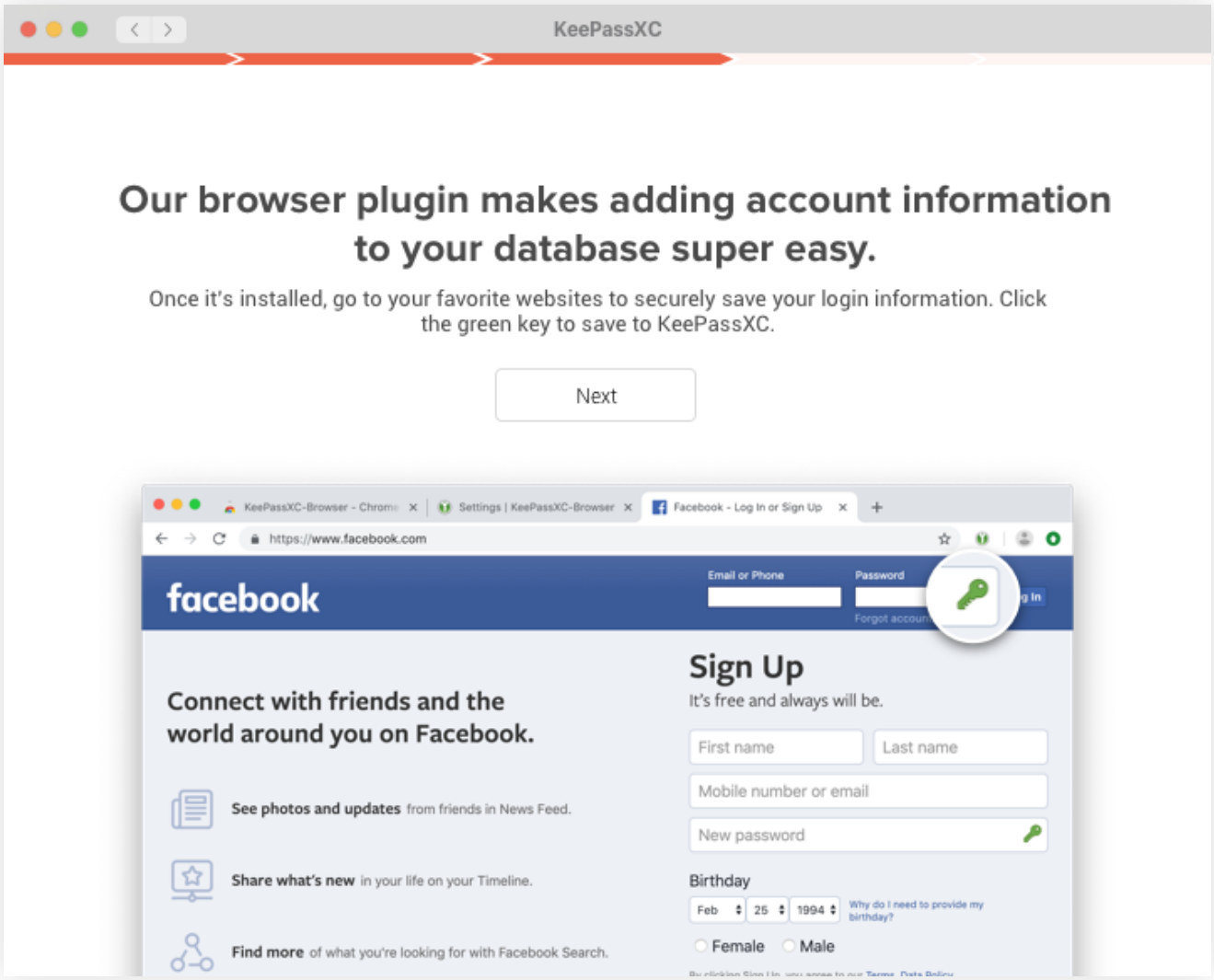
ONBOARD SCREEN 2

Create Database



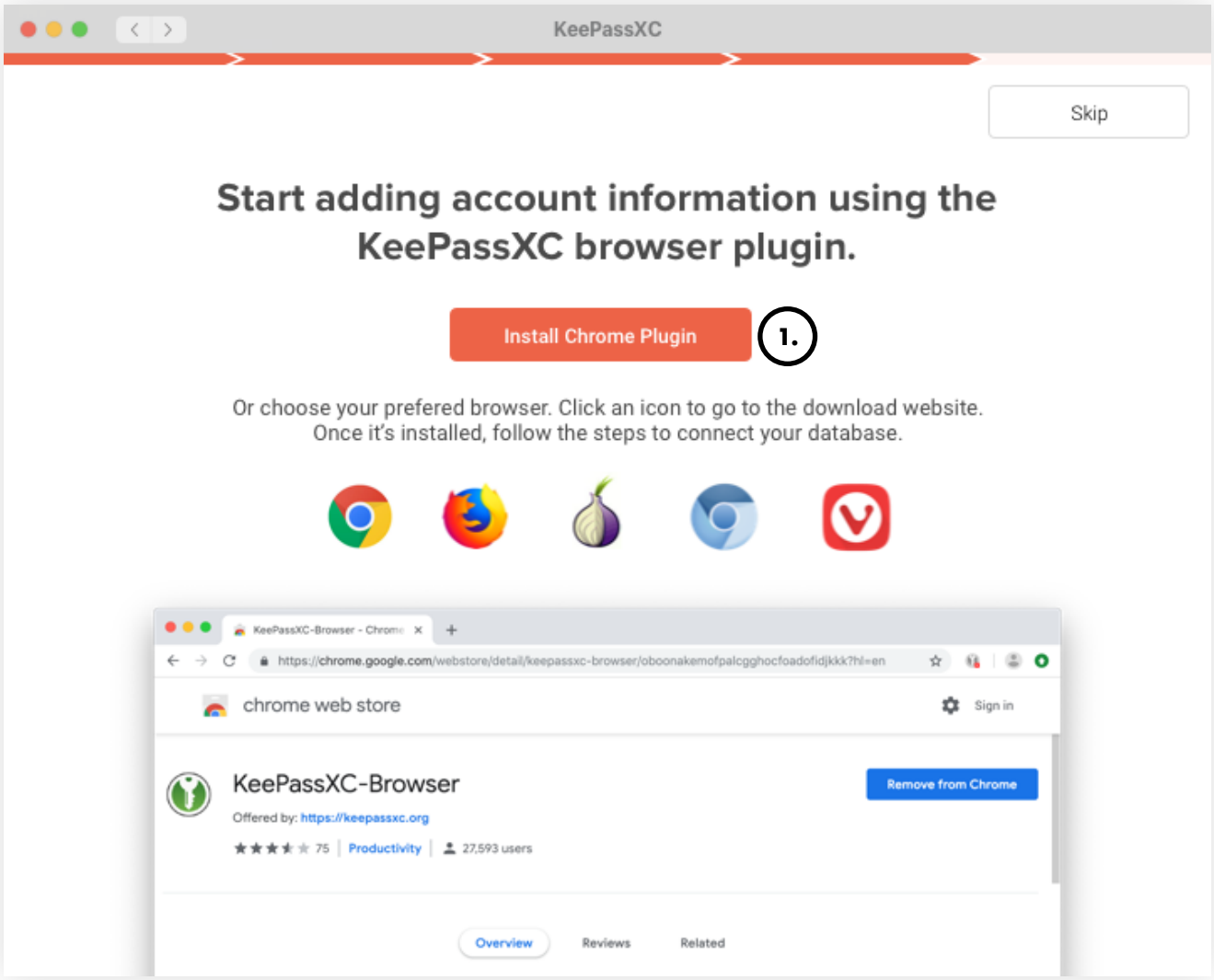
ONBOARD SCREEN 3

Plugin Pitch



ONBOARD SCREEN 4

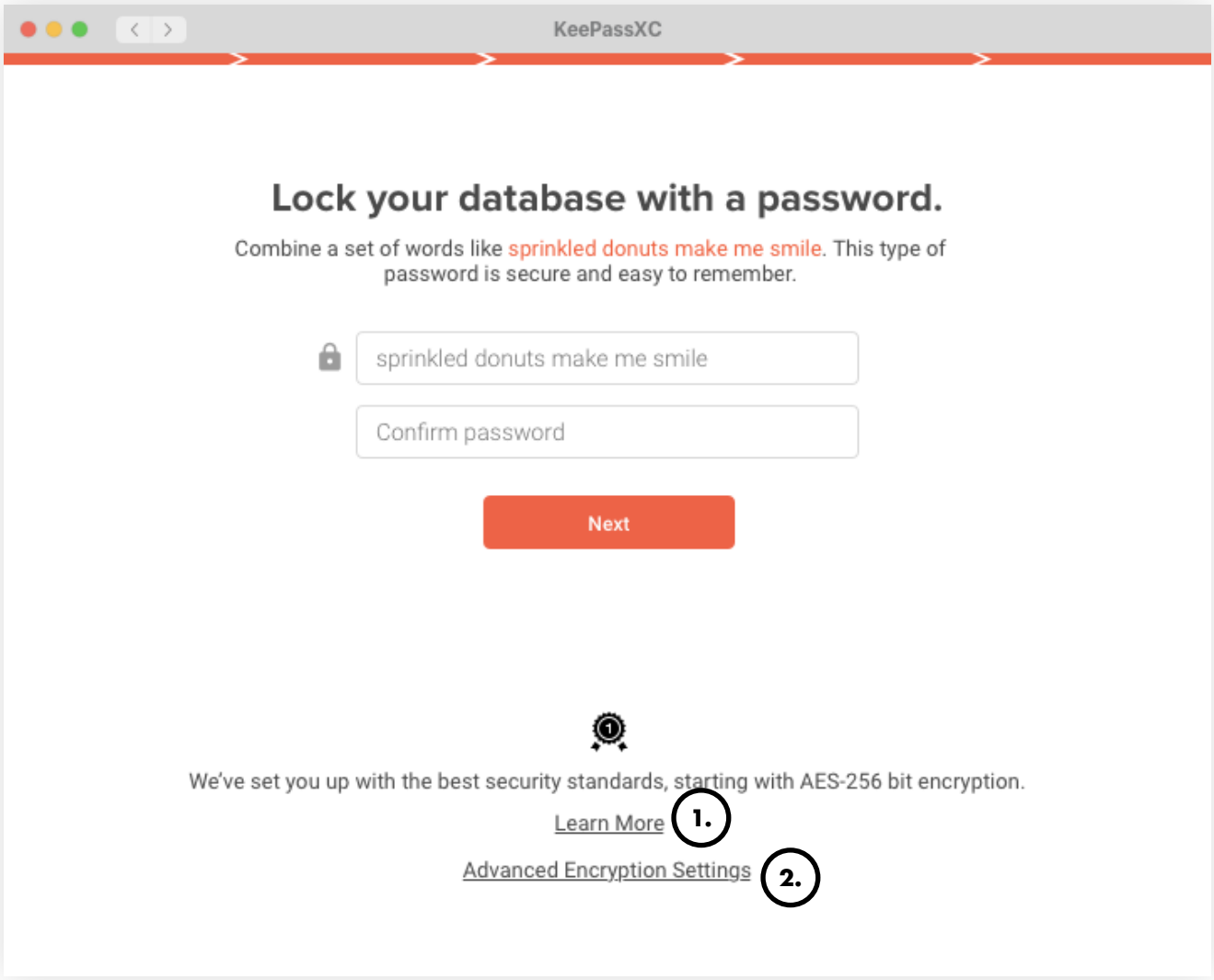
Install Plugin



1. Clicking “Install Chrome Plugin” opens the Chrome web store in the browser with the KeePassXC plugin featured

ONBOARD SCREEN 5

Set Database Password

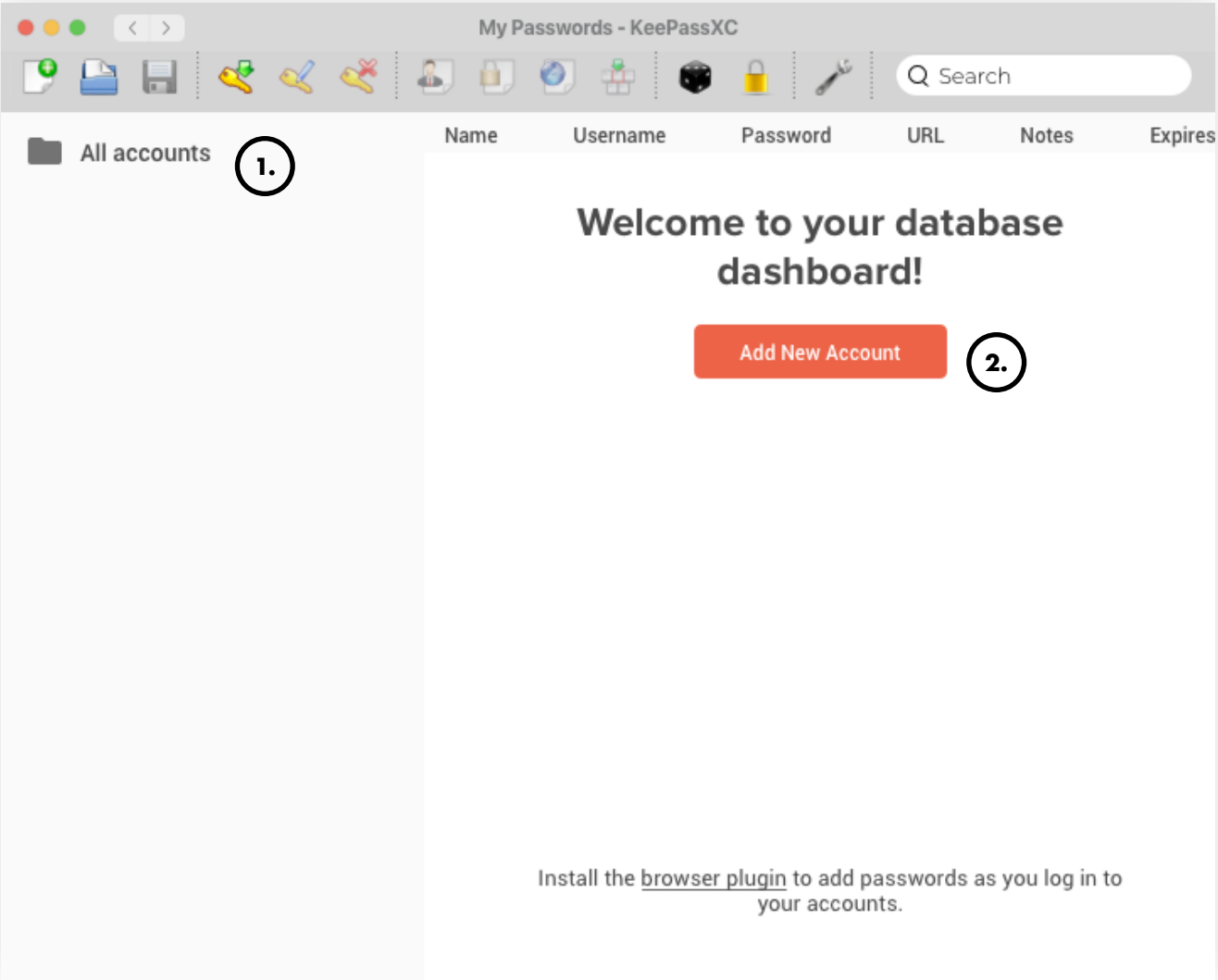


1. Clicking "Learn More" opens a webpage on KeePassXC's website that explains how it's secure in a very user-friendly fashion.

2. Clicking "Advanced Encryption Settings" takes the user to the current encryption settings view in the app.

ONBOARD SCREEN 6

Database Empty State: Add New Account

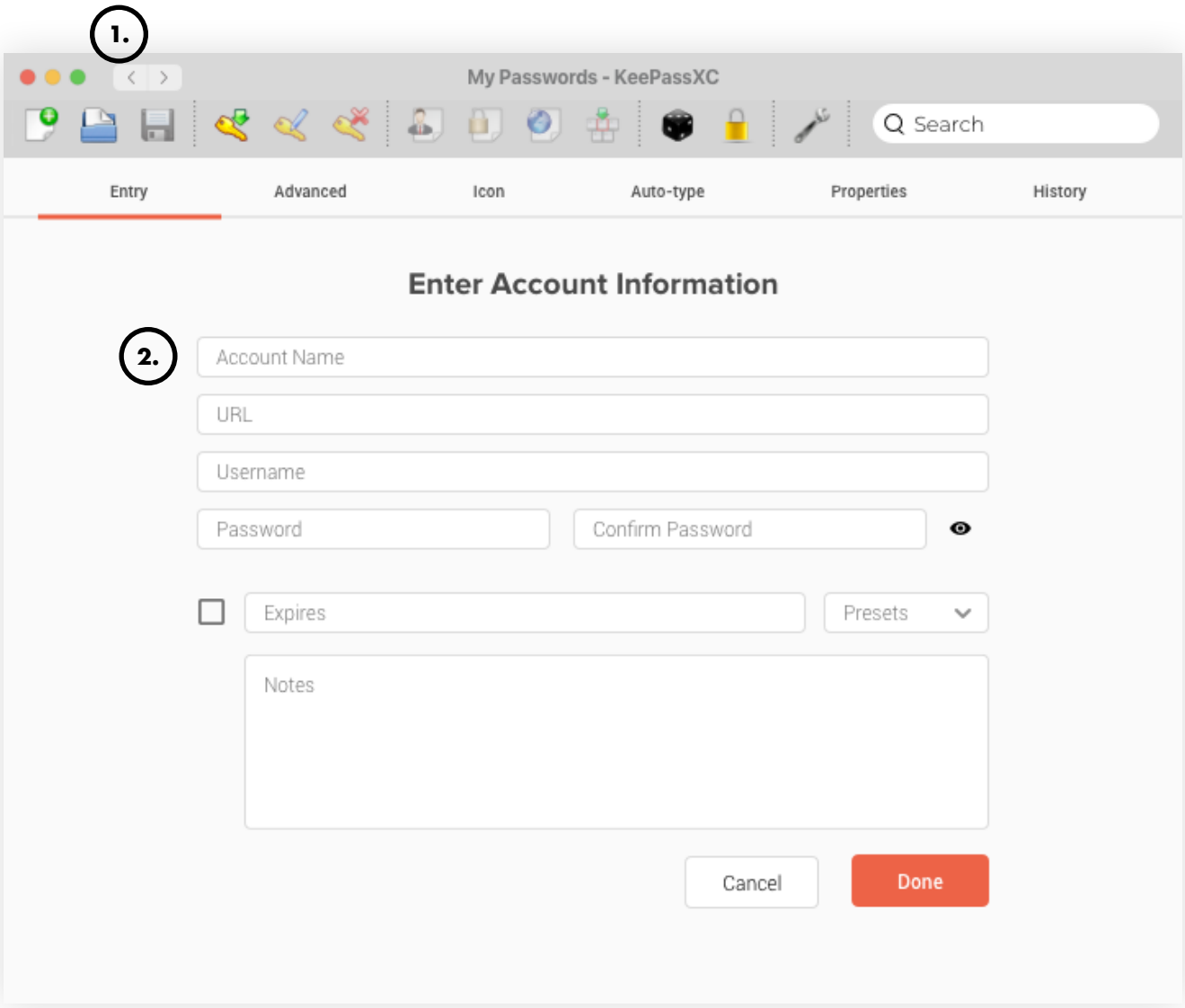


1. **NOTE:** We've changed "Root" to "All accounts" to make it easier to understand.

2. Clicking "Add New Account" takes the user to the new entry view.

ONBOARD SCREEN 7

Enter Account Information

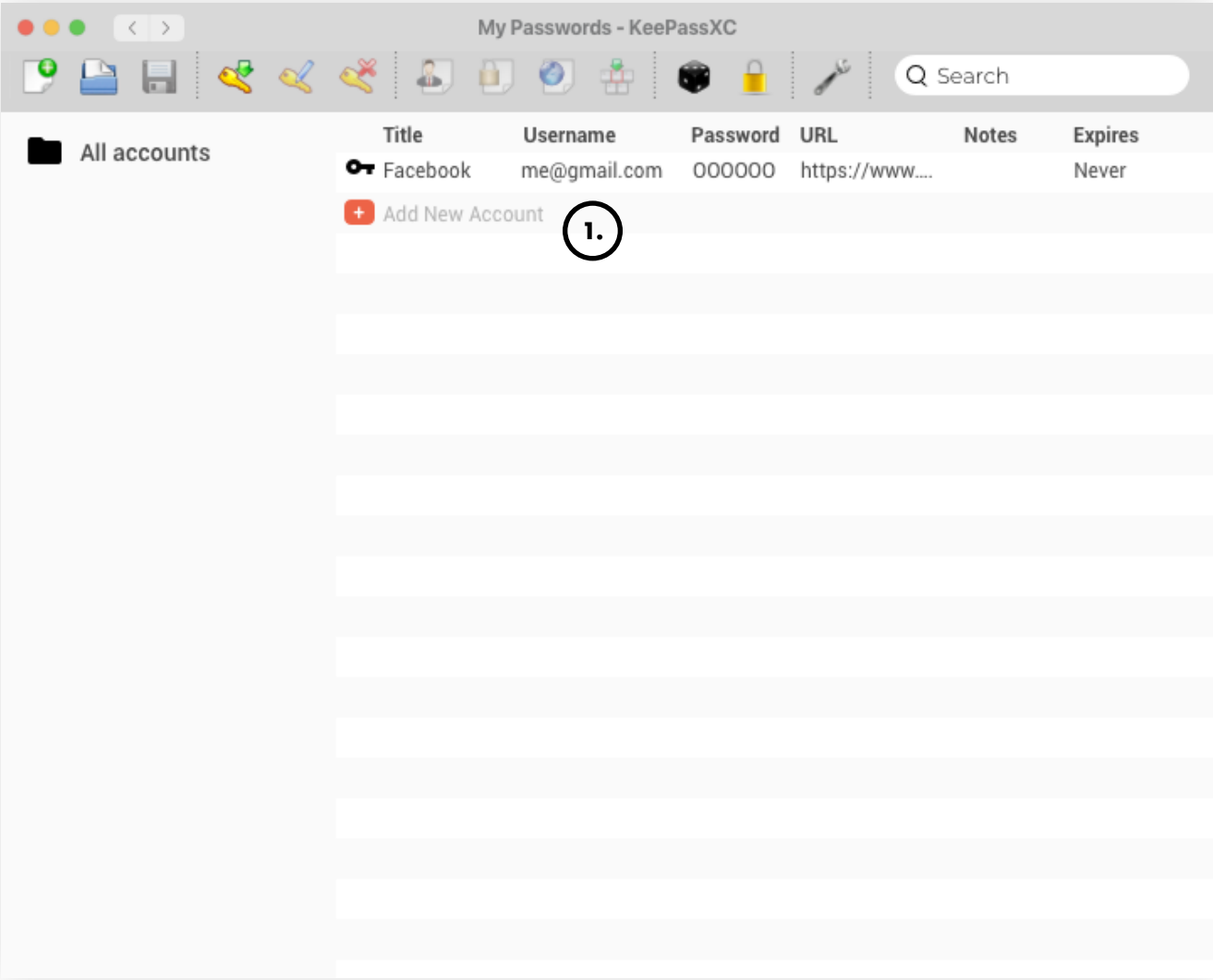


1. We recommend adding a back arrow that's native to the desktop app operating system.

2. We recommend re-ordering the input fields on the entry page to make it easier to comprehend.

ONBOARD SCREEN 8

Database With Entry



1. Clicking “Add New Account“ takes the user to the New Entry View.