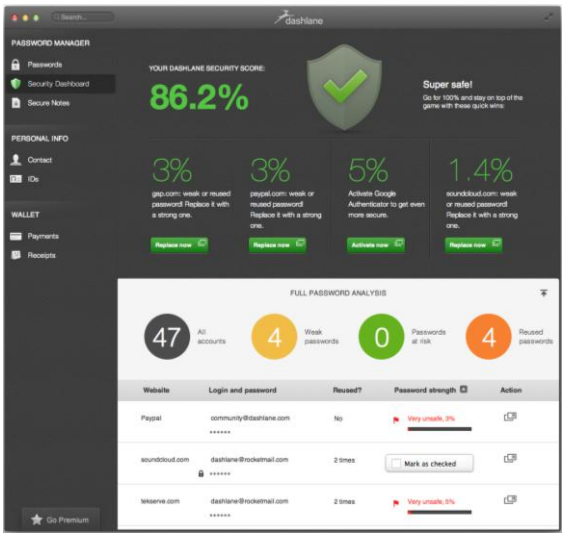
Dashlane 2.0 – FAQ

What's new in Dashlane 2.0?

With 2.0, our goal is to clearly establish Dashlane as the world's best password manager and secure digital wallet. We're paving the way on innovation, and also taking direct feedback from our users on what has worked and what hasn't. Here are the highlights:

- **Completely new design on PC & Mac**. We've improved color and contrast to make the app way easier on the eye. Our Mac app is now absolutely cutting edge in design/UX (fully responsive, subtle slides/springs that delight, etc.)
- **Whole new Security Dashboard, with a Security Score**. An easy-to-understand aggregate score for each user that provides an overall view of your password health. We also provide a customized list of easily digestible, top priority steps to improve your password security.
- **Massive jump in product quality**. Support for 2-step/3-field logins, other auto-login and autofill improvements, etc.
- **Totally new onboarding experience**. Incredibly in-line and intuitive way for new users to learn how to auto-login, autofill and use our app to the fullest.
- **2-factor authentication** via Google Authenticator on our desktop and mobile apps.
- **Android overhauled** (more about this below)
    - In-app browsing with full auto-login and autofill
    - Support for tablet and all screen-sizes
- **Points-based gamification dropped**. An interesting experiment, but we've learned from experience and feedback that it doesn't have a place in our app.
- **Silent updates**. Future updates for the desktop version of the product will now be made automatically.

A full set of screenshots are attached in the accompanying zip file.
Here's our new security dashboard!

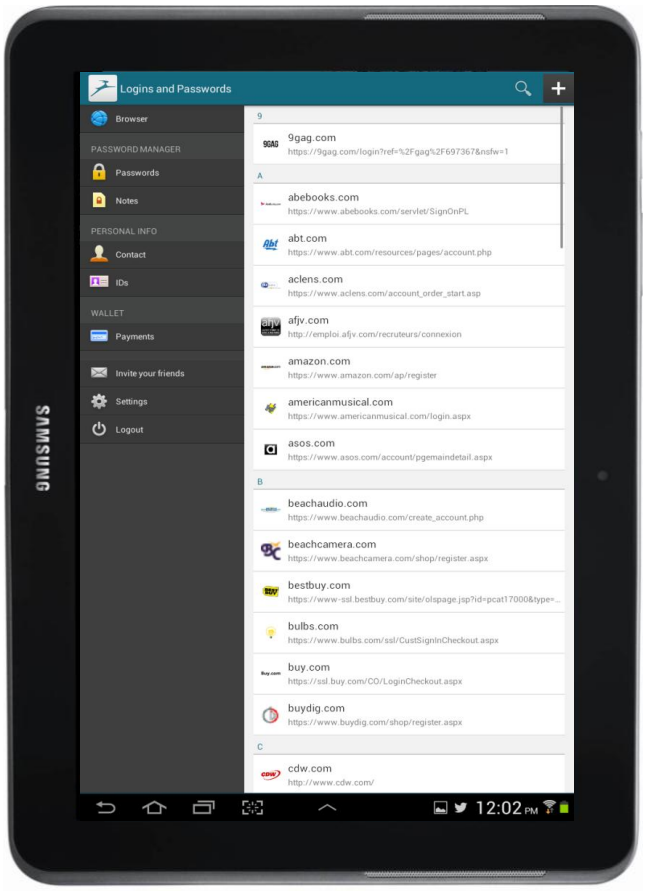


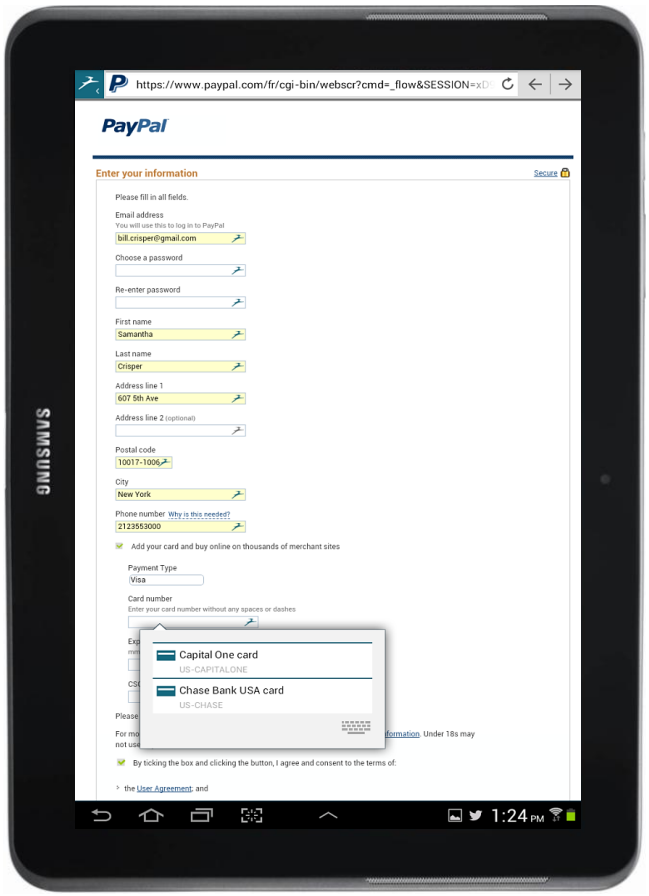
What's new in the Android version?

Our Android app's getting a full overhaul!

- **In-app browser:** A built-in browser that brings the most accurate auto-login and autofill technology to Android devices, including full Dashlane browser functionality as in our desktop apps!
- **Support for tablets and all screen sizes** with one universal app
- **UI focused for Android**: Our app has been completely re-designed using the Holo Interface
- **Two-factor authentication** via Google Authenticator

Check out the new Android app on tablet!

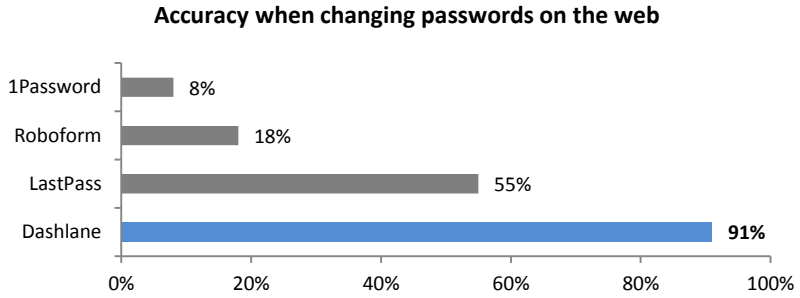




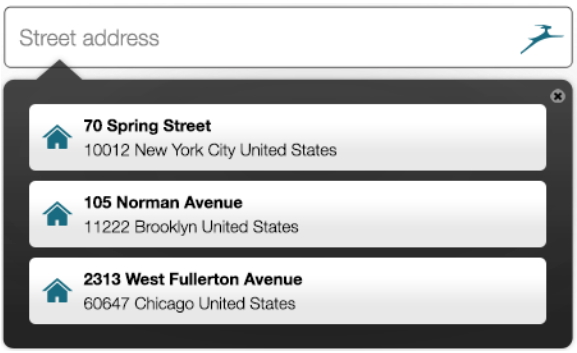
How is Dashlane different from the competition?

There are two major areas which set Dashlane apart from competing password managers.

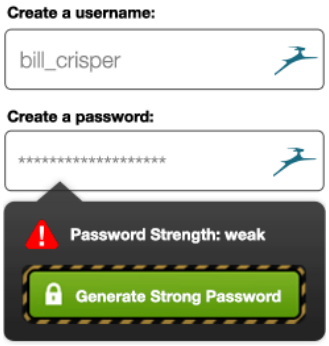
Significantly better product reliability: As documented in an unbiased benchmark study (attached with the zip file), Dashlane works significantly better than the competition for the basic features that one would expect from a password manager – capturing and changing passwords, auto-login without clicks, etc. Dashlane has spent over two years developing our proprietary semantic technology that has resulted in an autofill solution that is more accurate than any leading competitor.



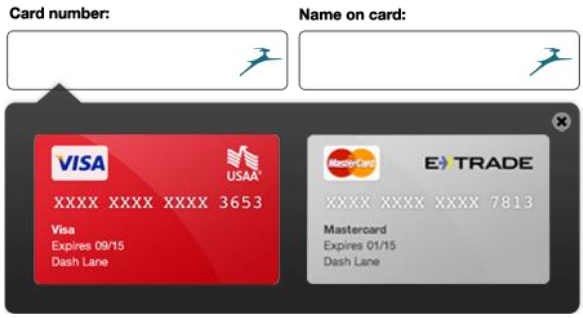
Massively better usability: Dashlane's user interaction happens right on the webpage within the browser, next to each form field. This "inline" method, without clunky toolbars, extra steps or other interruptions to web browsing, results in a far better experience for the user. We hold an incredibly high standard for simplicity of design and user experience, and are making our app for a much larger base than techies.



Autofill with Dashlane



Generating a password



Credit card autofill

What's happening with Dashlane Premium?

We're revising the list of features included in Dashlane Free vs. Dashlane Premium to be simpler, clearer, and more in line with user expectations. Our 2.0 Premium offering includes:

- Unlimited backup of encrypted data
- Automatic sync between devices
- Web access to logins and passwords
- Priority user support

…all for only $19.99 per year.

Remind me about Dashlane's security model?

- **AES-256 encryption**: Every user's data is encrypted with AES-256 (the world's leading standard), with 10,000+ rounds of PBKDF2 salt. Open source yet remains uncracked. Widely accepted as the strongest, and NSA-Certified.
- **Encryption keys are NEVER recorded:** The key that encrypts our users' data is derived from their master password. There is NO RECORD of either the master password or this derived key anywhere in the universe - not on their device, not on our servers, nothing transmitted on the web.
- **Local-only or seamlessly synced:** Users can choose to have their private, encrypted data never leave their device. Or, they can seamlessly sync their data (AES-256 encrypted, of course,) via our servers to multiple devices.
- **Two-factor authentication:** via Google Authenticator, to bring yet another layer of security to access data.

Dashlane doesn't need master passwords to authenticate our users. We authenticate them based on their machines, and this is initiated via a token sent to their email. Users use their master password post-authentication only to decrypt their data locally on their device.

Any user data in our cloud is always encrypted with AES-256, and always with a key completely unknown to us that is never stored or transmitted anywhere. Even if this data ever gets into the hands of anyone, it is pointless garbage given that each user's encrypted file would need to be brute-forced separately.

Because we never store even a derivative of the master password, we cannot recover a user's data if they forget their password – they need to start over with Dashlane. Our users understand that this is the only way for us to ensure that their data is inaccessible to anyone but them.

For full detail, please see our whitepaper here.

And your data privacy model?

- **Every bit of personal data entered into Dashlane is completely unreadable to us**, because it is encrypted with AES-256, and the encryption key is derived from the master password which is completely unknown to us.
- **If sync is enabled on an account, ONLY encrypted data is transmitted** to us to allow syncing. This synced encrypted data that we have cannot be directly linked back to any user, and is never shared. If sync is disabled, the encrypted data is only stored on the user's device, and any data that was previously synced to our servers is destroyed.
- **The only personal information we have on our users is their email address** (and their mobile phone number if they chose to give it to us for security purposes when they created their account.) We use this to communicate with users about their account. This information is NEVER shared unless users explicitly ask for it.
- **We collect technical and usage data to analyze how our product performs**, and for us to improve the quality of Dashlane. This data is completely anonymized except for gender, birth year and zip code, and cannot IN ANY WAY be linked to any user individual personal information – not even the email address they registered with us.

Our detailed privacy policy is here.

I have such-and-such gripe with Dashlane:

- **Where's my iPad app?** We're actively working on it, and you will not be disappointed. It should be out in a few weeks.
- **Where's my Linux version?** We're always trying to prioritize as a startup, and given what's in front of us, Linux is not on our roadmap yet. We will let you know when it is!
- **Do you work in-app yet?** Not yet, but we're actively investigating logins for mobile apps!
- **Why both an app and a browser extension?** Because user experience and user trust were our top concerns.
    - From our usability tests, we found that users feel more secure by entering their information into a desktop app vs. a browser
    - This enables us to securely provide our users with that "inline" user experience without having to go to a separate toolbar to auto-login or autofill
    - You can read more about this here: http://www.dashlane.com/blog/2011/07/18/desktop-app-or-web-app/
- **Where's support for languages beyond English and French?** Semantic technology needs to be developed for each additional language that is supported. A couple more should be coming in the next few months!