Throwing the Deadbolt on Internet Security

To-Do Items After Converting to 1Password

Making the move to use 1Password to manage your Internet logins is a big first step toward good Internet security practices. But if all you do with 1Password is use it to remember and fill in your Web logins, you're leaving several other potential vulnerabilities still open to compromise. 1Password can help you close these remaining attack vectors.

Setting up 1Password with the sync of your 1Password keychain to a cloud-based sync service like DropBox is the first step. With that in place, you have the following strong protections: your Web logins are stored in an encrypted database and not on paper or an insecure data file, and you have protection from keyloggers, phishing attacks and shoulder surfers.

That's a really good start, and much better than the large majority of Internet users will ever have. But with just a little extra effort, you can tighten down your Internet security to the point where essentially all attack vectors have been secured.

- **Delete** the stored credit card info on all retailer sites. Visit all the sites where you shop online and delete your credit card information from their system. 1Password will instantly and securely fill in your credit card info at the second it's needed, so there's no sense in risking a leak of your credit card info from a merchant site.
- To eliminate the need to keep a credit card on file with the iTunes store, **delete** your credit card info in your iTunes account if you have it on file, then buy iTunes gift cards at any retail store. Deposit the stored value of the card into your iTunes account using the "Redeem" link on the iTunes Store home page. You can do the same with other merchants by using gift cards, also available in the gift card rack at most retail stores. This prevents your credit card information from ever being susceptible to security breaches at any online merchant.
- Change the settings in all your Web browsers to **not remember** passwords and logins. 1Password is all you need, and leaving stored passwords and logins stored in your browser is an unnecessary security risk. In Safari, choose Preferences from the Safari menu, then click the Autofill tab., then un-check all the options.
- Delete all the Web logins from your Mac's Keychain file. Open the Keychain Access utility in your Utilities folder. Click "All Items" in the Category pane at bottom left, then use the search box at top right to search for the domains of any sites that you now use 1Password to log into. When you find one, confirm that the "Kind" column reads "Internet password" or "Web form," and then press the delete key to delete it.
- Use 1Password to visit and log into the sites that have your most sensitive banking, credit card, finance, investment and medical information. Then use the "Generate strong password" feature of 1Password to generate a new, strong, random password for each site. When 1Password prompts you to store the new password, select "Replace (name of login)" from the pop-up menu to update 1Password with the new, secure password.
- Use the "Secure Notes" feature in 1Password to keep all your important info in one safe, encrypted place. Remember, you can drag attachments into any 1Password item, so keep copies of your will, insurance policies, health records, important receipts, warranty info, etc., as attachments in the related 1Password item.
- Make a habit of using the "Wallet" and "Software" categories in 1Password for your software license info, credit card and bank account info, safe deposit box info, passport and drivers license info, and anything else you'd like to keep safe, secure and instantly available when you need it, anywhere.
- Use the "1Password Anywhere" feature of 1Password in a DropBox folder to access your 1Password data from any Internet-connected computer.
- Before you leave on a trip, drag a copy of your 1Password keychain onto a USB thumb drive to carry with you...just in case. The 1Password data file is encrypted, so there's no need to worry if the drive is lost or stolen.