

Throwing the Deadbolt on Internet Security

To-Do Items After Converting to IPassword

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

Setting up IPassword with the sync of your IPassword 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. IPassword will instantly and securely fill in your credit card info when 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 prepaid Amex 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.
- 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 IPassword 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 IPassword 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 IPassword to generate a new, strong, random password for each site. When IPassword prompts you to store the new password, select "Replace (name of login)" from the pop-up menu to update IPassword with the new, secure password.
- Use the "Secure Notes" feature in IPassword to keep all your important info in one safe, encrypted place. Remember, you can drag attachments into any IPassword item, so keep copies of your will, insurance policies, health records, important receipts, warranty info, etc., as attachments in the related IPassword item.
- Make a habit of using the "Wallet" and "Software" categories in IPassword for your software license info, credit card and bank account info, safe deposit box info, and anything else you'd like to keep safe, handy and secure.
- Use the Wi-Fi sync feature of IPassword to keep an updated mobile copy of all your IPassword data on your iPhone, iPod Touch or iPad.
- Use the "IPassword Anywhere" feature of IPassword in a DropBox folder to access your IPassword data from any Internet-connected computer.
- Before you leave on a trip, make a copy of your IPassword keychain on a USB thumb drive to carry with you...just in case.