Password Management

1. LastPast: LastPast makes it easy to audit your passwords, use stronger passwords in general, and even automatically change a password for you if a service has been hacked or compromised. LastPast supports two-factor authentication for your password vault using Google Authenticator, USB devices, or a YubiKey, The service picked up a much-needed update a year or so ago to streamline the UI and make it easier to use, and sports a number of additional features like credit monitoring, secure password and document storage (and sharing), notifications when a site you have an account with has been hacked, tools to autofill forms and streamline online shopping, and more. It's free to download and use, but if you want its best features and the mobile apps, you'll need to upgrade to LastPast Premium, at $12/yr.
2. Dashlane: Dashlane provides simple security, easy auto-login, form auto-fill, and logging of purchases and orders from online shops. It’s supporting of two-factor authentication, the ability to share passwords with emergency contacts in case you can't access your accounts along with giving you the ability to change multiple passwords on dozens of websites with a few clicks. Dashlane will also notify you if you have an account on a site that's hacked, and with its built-in password changer, you can have Dashlane reset the password to a new, unique, strong one without leaving the interface. The purchase tracking and digital wallet features make it easy to make online purchases even at retailers you don't have accounts with, and search all of your online orders in one place. Dashlane also gives you the option to store your passwords locally only in an encrypted vault (where only you have the master key), or to sync them to your devices and access them on the web. It's free to download and use, but if you want your passwords synced across devices, you'll need Dashlane Premium, at $40/yr.
3. KeePass: KeePass is a portable app, meaning it's super easy to take with you and use on multiple computers. It has its own password generator, to help you change passwords and make sure every one of them is unique and strong. Passwords database in KeePass can be configured with multiple keys, so you can share access among privileged users, and exported in plain text for quick importing elsewhere. KeePass has tons of third-party plugins and tools to extend its functionality and bring it to more devices, browsers, and platforms. You can put all your passwords in one database, which is locked with one master key or a key file. You only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish). Keypass is free to use.
4. 1Password: 1Password can be used locally only, without syncing any information to the web, or you can use it across all of your devices by syncing your encrypted vault via Dropbox, iCloud, Wi-Fi, or shared network folders. You can also set up emergency contacts and share passwords with authorized users. You can even keep multiple vaults for different types of passwords. 1Password supports Windows, OS X, Android, and iOS, with plugins for Chrome, Firefox, Opera, and Safari. The prices for 1Password varies.
5. RoboForm: Roboform gives you the option to keep your passwords and data encrypted and local, or sync to the web and across devices. It supports multiple identities, so you can autofill form information based on different users, addresses, or any other mix-and-match of data you choose. You can also take RoboForm with you on a USB drive from computer to computer. Additionally, it integrates with IE, Firefox, Chrome on Windows as well as Chrome and Safari for Macs, allowing you to share info between browsers and making your web experience faster, easier and more secure. Currently, Roboform can be bought for $9.99 for the first year.