INFORMATION SECURITY GUIDELINE

Password Safes

Introduction

1. Password Safes (or Password Managers) are computer applications that provide a secure place to store and access the passwords/passphrases for different login environments. Password Safes are simple to use because they can be accessed with a single master password/passphrase.
2. This guideline has been issued by the Chief Information Officer to supplement the Password and Passphrase Protection standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Master Passwords/Passphrases

3. The master password/passphrase used to protect the Password Safe must be strong; otherwise the security of the safe and all of its contents are at risk. Refer to the Password and Passphrase Protection standard for information on how to design a secure password/passphrase.
4. The master password/passphrase must be changed at least annually.
5. Users are responsible for remembering the master password/passphrase. If it is lost or forgotten, UBC cannot recover or bypass it.

Types of Password Safes

6. Picking a Password Safe can be tricky. Here is a summary of the available options:

Type	Description	Notes
Standalone	These are installed on the desktop or on your mobile device as an application.	With these services, the data is accessible no matter if an internet connection is available or not. However, if the device is lost or the database corrupted, then the only way to recover the data will be through a backup copy.
Web-based	These are accessible through a web browser and are stored online as part of a cloud service.	With these services, the data is not susceptible to database corruption or loss of the device. However if the site is inaccessible or no Internet connection is available, then the passwords will not be accessible.
Web-browser-based	Most web browsers have the ability to "Remember this password" for secure login sites.	Using these services is not recommended. Browsers are subject to constant attack and there are known vulnerabilities that can expose passwords stored in browsers. Many of the premium password safes now offer to import the browser passwords lists, leading to a faster start-up time.
Mixed	Newer services offer a dual environment, with device-based apps that are synched to the cloud.	These combine the benefits of standalone and web-based systems.

Current Leading Password Safes

7. Here are some of the leading Password Safes:

Name	Description	Link to More Information
KeePass	A popular open-source, cross-platform, desktop-based password manager. It is available for Windows, Linux and Mac OS X as well as mobile operating systems like iOS and Android. It stores all passwords in a single database (or a single file) that is protected and locked with one master key. The database is encrypted using the best and most secure encryption algorithms currently known (AES and Twofish). The database can be stored on a cloud drive (e.g. Workspace), which is then accessible across multiple devices. (Recommended)	http://keepass.info/help/base/firststeps.html Type: Standalone. Can be used as Mixed.

Name	Description	Link to More Information
LastPass	Available for Windows, Mac, and Linux (and iOS, Android, and Windows). Once the master password has been setup, LastPass will import all saved login credentials (usernames and passwords) from Firefox, Chrome, Internet Explorer, Opera, and Safari. It then prompts for deletion of all of this information from the computer to keep it secure. LastPass for mobile will require a premium subscription fee.	https://lastpass.com/support.php?cmd=getfeaturefaq&feature=feataure_0 Type: Web-based
RoboForm	Another password manager, as well as a tool to automatically fill in online forms. RoboForm is available for Windows, Mac, iOS, and Android. RoboForm stores information locally, rather than in the cloud. A subscription service is available, RoboForm Everywhere, which will upload a User's data to the cloud and making it available across multiple platforms.	http://www.roboform.com/tutorials Type: Standalone. Can be upgraded to Mixed.
My1login	A robust web-based password manager that is free for individuals. It offers the ability to memorize all online web login information by adding simple bookmarks to a web browser. My1login is not available as a mobile application.	Type: Web-based

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Password and Passphrase Protection standard