

Copyright (C) 2023- mirage335
See the end of the file for license conditions.
See license.txt for credManager license conditions.

Integrates other password managers, plain text records, with reporting and mismatch detection.

Template credentials records for an individual user are provided as text files under the 'self' directory.

Example exported password CSV files are provided under the '_ref/import/export' directory.

Example reporting scripts are provided under the '_ref/report' directory . These will output '.pdf' and '.sh.out.txt' files of the same name as appropriate.

Quad-Redundant/BTRFS Magneto-Optical single-layer (NOT Gigamo) discs and frequent write-once optical disc (ie. modern M-Disc) backups are strongly recommended. Such discs may be created, and backup discs derived, using 'flipKey' . Such optical storage has far better longevity and reliability than such other storage as USB Flash, SDCards, SSDs, HDDs, etc. Write-once backups set aside mitigate erasure by malware.

Strong 2FA (ie. redundant hardware FIDO/U2F, FIDO2) is very strongly recommended. Other authentication (eg. recovery codes, TOTP, non-standalone passkeys) relies on the confidentiality and/or integrity of modern computers, operating systems, etc, which now have far too large an attack surface (including Spectre, Meltdown, BadUSB, vulnerable networks, etc - malware).

Examples

This repository itself is an example.

Usage

```
find . -name "*.sh" -exec {} \;
```

Design

Self-modifying credManager scripts generate text/shell, and HTML to PDF, output.

Safety

Strong 2FA is now necessary. Do NOT trust recovery codes . Do NOT trust TOTP . Do NOT trust passwords. Do NOT trust non-standalone (ie. other than YubiKey Bio) platform keys.

Do NOT trust any authentication ever visible to the host.

Plan for what to do after malware has compromised all sessions for any password reset channel (eg. email).

Integrity or Availability relying on the Confidentiality of modern computers, operating systems, etc, WILL fail.

Use only FIDO/U2F with multiple redundant standalone hardware security keys (ie. YubiKey), or better (ie. FIDO2).

PASSWORDS ARE NOT SAFE. YOU HAVE BEEN WARNED.

Reference

Copyright

This file is part of credManager.

credManager is free software: you can redistribute it and/or modify it under the terms of the Affero GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

credManager is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the Affero GNU General Public License for more details.

You should have received a copy of the Affero GNU General Public License along with credManager. If not, see <<http://www.gnu.org/licenses/>>.