Anleitung

1. Allgemeines

MyLastKey wurde entwickelt, um eine zuverlässige, sichere und übersichtliche Software zur Aufbewahrung von:

- Passwörtern und Zugangsdaten
- Orte von Verstecken
- Geheimnissen
- Rezepturen
- Tresor-Kombinationen
- Seeds und Keys für Kryptowährungen
- Adressen von wichtigen Personen und Unternehmen
- Kundennummern (bspw. Rentenversicherung)
- anderen sensiblen Daten

anzubieten.

Aus Sicherheitsgründen ist es ratsam, die MyLastKey-Software auf einem USB-Stick zu installieren und die Zugangsdaten und den USB-Stick in einem Tresor aufzubewahren.

2. Innovation

Der innovativste Vorteil von MyLastKey ist, dass Sie Ihre Zugangsdaten zur MyLastKey-Software **nicht** zwingend zu Lebzeiten an eine Vertrauensperson weitergeben müssen oder handschriftlich, also unverschlüsselt, hinterlegen müssen.

MyLastKey schützt Ihre sensiblen Daten und Geheimnisse bestmöglich vor **unberechtigtem Zugriff**, wie bspw. durch Einbrecher, Erbschleicher oder der Regierungsorganisationen, durch den **MyLastKey „KeyPass"**.
Mehr Infos zum KeyPass unter Punkt 4.5.

3. Login-Maske

3.1 Erstmalige Nutzung

- Wenn Sie MyLastKey erstmalig nutzen, brauchen Sie lediglich den Button „Start" zu drücken. Die Standard-Zugangsdaten lauten: „MyLastKey!".

3.2 Werkseinstellungen

- Hier können Sie die gesamte Software auf Werkseinstellungen zurücksetzen.
- Bitte beachten Sie, dass sämtliche Daten, die bisher erfasst wurden, verloren gehen.

3.3 Wallet importieren und exportieren

- Unter diesen Buttons können Sie eine Wallet importieren oder exportieren.
- Wenn Sie eine Wallet importieren möchten, dann wird die aktuelle Wallet sicherheitshalber im Ordner „/Logs" als Backup abgespeichert.
- Wenn Sie eine Wallet exportieren (Backup) möchten, dann werden die Verzeichnisse „Config" und „Filesafe" in zwei ZIP-Dateien exportiert. Wenn Sie dieses Backup wieder importieren möchten, dann müssen Sie die Backup-ZIP-Dateien zuerst entpacken und dann die Wallet importieren.
- Die Filesafe-Dateien werden aus Sicherheitsgründen nicht automatisch importiert. Diese können Sie bei Bedarf in den Ordner „Filesafe" kopieren.
- Unter dem Punkt „Backup Cloud" können Sie einen eingebundenen Dropbox- oder OneDrive-Ordner auswählen. Bei jeder Änderung wird hier eine verschlüsselte Backup-Datei abgelegt.

3.4 Assistent wieder aktivieren

- Beim erstmaligen Einrichten von MyLastKey wird der „Eingabeassistent" automatisch aktiviert, der Sie durch die ersten Einstellungen führt.
- Unter diesem Punkt können Sie diesen nachträglich wieder aktivieren.

3.5 Entschlüsselung

- Unter diesem Punkt können Sie eine Entschlüsselung der Wallet beantragen.
- Das weitere Vorgehen wird dort beschrieben.

4. Hauptmaske

4.1 Eingabefeld (Passwörter / Banken / Adressen / Sonstiges)

- In den Eingabefeldern können Sie Ihre Daten unbegrenzt abspeichern.
- In den Eingabefeldern können Sie mit der Tastenkombination „Shift + Enter" einen Zeilenumbruch einfügen.
- Eine Zeile können Sie löschen, in dem Sie die Zeile markieren und die Taste „Entfernen" drücken oder das Kontextmenü (rechte Maustaste) aufrufen.

4.2 Dateisafe

- Der Dateisafe befindet sich im Ordner „/Filesafe".
- Hier können Sie Dokumente, wie bspw. Ihr Testament verschlüsselt abspeichern.
- Die verschlüsselten Dateien erhalten die Dateiendung *.encrypt.
- Es wird lediglich eine Kopie der Original-Datei verschlüsselt. Die Original-Datei bleibt unverändert.
- Bei Bedarf können Sie die Dateien wieder entschlüsseln.

4.3 Benutzernamen und Passwort ändern

- Sie können beliebig oft das Passwort ändern.
- Das Passwort muss mindestens 10 Stellen betragen.

4.4 Export

- Aus Sicherheitsgründen wird kein Export der Daten angeboten.
- Hierdurch werden Hackerangriffe und Phishingversuche erschwert.
- Sie können auf eigenes Risiko die Tabellen markieren (STRG+A) und kopieren (STRG+C) und dann in eine Excel-Tabelle einfügen.

4.5 KeyPass

- Hier können Sie einen **KeyPass** für Vertrauenspersonen ausstellen.
- Tragen Sie als erstes Ihren Vor- und Nachnamen, die Adresse, die PLZ und den Wohnort ein.
- Anschließend tragen Sie diese Daten auch für die Vertrauensperson ein.
- Über den Button „**PW verschlüsseln**" können Sie das Passwort für die MyLastKey-Software verschlüsseln.

- Die Vertrauensperson kann nur gegen Vorlage des **KeyPasses, eines Personalausweises und ggfs. eines Erbscheins** eine Entschlüsselung unter service@mylastkey.com beantragen.
- Nur wenn die Vertrauensperson alle Dokumente vorlegt, werden wir Ihre **Zugangsdaten** zur MyLastKey-Software entschlüsseln und herausgegeben.
- **Wichtig: Unser Unternehmen entschlüsselt lediglich das Passwort. Wir bekommen zu keiner Zeit Zugriff auf Ihre Daten und Geheimnisse.**

5. Kontaktdaten

Decrypta Technologies GmbH
Gillstr. 30
58239 Schwerte
Germany

office@mylastkey.com