Instruccio

1. Generalidades

MyLastKey fue desarrollado para proporcionar un software fiable, seguro y claro para almacenar:

- contraseñas y datos de acceso
- ubicaciones de escondites
- secretos
- recetas
- combinaciones de bóvedas
- Semillas y claves para criptomonedas
- Direcciones de personas y empresas importantes
- Números de clientes (por ejemplo, seguros de pensiones)
- otros datos sensibles

otros datos sensibles.

Por razones de seguridad, se recomienda instalar el software MyLastKey en una memoria USB y guardar los datos de acceso y la memoria USB en una caja fuerte.

2 Innovación

La ventaja más innovadora de MyLastKey es que usted no tiene que transmitir en vida sus datos de acceso al software MyLastKey a una persona de confianza ni depositarlos a mano, es decir, sin cifrar.

MyLastKey protege sus datos sensibles y secretos de la mejor manera posible contra el acceso no autorizado, como por ejemplo por parte de ladrones, cazadores de legados u organizaciones gubernamentales, a través del pasaporte MyLastKey.

Encontrará más información sobre el pasaporte MyLastKey en el punto 4.5.

También puede utilizar MyLastKey como software gestor de contraseñas. En cuanto haya seleccionado un campo, el contenido se copiará automáticamente en la caché, de modo que sólo tendrá que pegar el

nombre de usuario o la contraseña en una página de Internet con (CTRL+V).

3 Máscara de inicio de sesión

3.1 Primera utilización

- Si es la primera vez que utiliza MyLastKey, sólo tiene que pulsar el botón "Iniciar". Los datos de acceso por defecto son: MyLastKey!

3.2 Configuración de fábrica

- Aquí puede restablecer todo el software a los ajustes de fábrica.

- Tenga en cuenta que se perderán todos los datos registrados anteriormente.

3.3 Importar y exportar monedero

- En estos puntos puede importar o exportar un monedero.

- Si desea importar un monedero, el monedero actual se guarda como copia de seguridad en la carpeta "/Logs".

- Si desea exportar (Backup) un monedero, los directorios "Config" y "Filesafe" se exportan en dos archivos ZIP. Si desea volver a importar esta copia de seguridad, primero debe descomprimir los archivos ZIP de copia de seguridad y, a continuación, importar el monedero.

- Los archivos "Filesafe" no se importan automáticamente por razones de seguridad. Si es necesario, puede copiarlos en la carpeta "Filesafe".

- En "Backup Cloud" puede seleccionar una carpeta integrada Dropbox o OneDrive. Con cada cambio, aquí se almacena un "archivo de copia de seguridad" encriptado.

3.4 Reactivar Asistente

- Cuando configura MyLastKey por primera vez, el asistente de entrada se activa automáticamente y le guía a través de los ajustes iniciales.

- Puede reactivarlo más tarde en este punto.

3.5 Descifrado

- En este punto puede solicitar la desencriptación del monedero.

- Allí se describe el procedimiento posterior.

4. pantalla principal

4.1 Campo de entrada (Contraseñas / Bancos / Otros)

- Puede guardar sus datos en los campos de entrada por tiempo ilimitado.

- En los campos de entrada puede introducir una línea con la combinación de teclas "Shift+Enter" para insertar un salto de línea.

- Puede borrar una línea marcándola y pulsando la tecla "Delete".

4.2 Caja fuerte

- La caja fuerte de archivos se encuentra en la carpeta "/Filesafe".

- Aquí puedes guardar documentos, como tu testamento, de forma encriptada.

- Los archivos encriptados tienen la extensión *.encrypt.

- Sólo se cifra una copia del archivo original. El archivo original permanece inalterado.

- En caso necesario, puede volver a descifrar los archivos.

4.3 Cambiar el nombre de usuario y la contraseña

- Puedes cambiar la contraseña tantas veces como quieras.

- La contraseña debe tener al menos 10 dígitos.

4.4 Exportación

- Por razones de seguridad, no se ofrece la posibilidad de exportar los datos.

- Esto dificulta los ataques de hackers y los intentos de phishing.

- Por su cuenta y riesgo, puede seleccionar (CTRL+A) y copiar (CTRL+C) las tablas y luego pegarlas en una hoja de cálculo Excel.

4.5 KeyPass

- Aquí puede emitir un KeyPass para personas de confianza.

- Introduzca primero su nombre y apellidos, dirección, código postal y lugar de residencia.

- A continuación, introduzca también estos datos para el tercero de confianza.

- Puede cifrar su contraseña para el software MyLastKey utilizando el botón "Cifrar PW".

- El tercero de confianza sólo puede solicitar el descifrado presentando el KeyPass, un documento de identidad y, en su caso, un certificado de herencia en service@mylastkey.com.

- Sólo si la persona de confianza presenta todos los documentos descifraremos y emitiremos sus datos de acceso al software MyLastKey.

- Importante: Nuestra empresa sólo descifrará su nombre de usuario y contraseña. En ningún momento tendremos acceso a sus datos y secretos.

5. datos de contacto

Decrypta Technologies GmbH
Gillstr. 30
58239 Schwerte
Alemania

office@mylastkey.com