

F-SECURE ID-PROTECTION

Schritt für Schritt erklärt

Inhalt

Was ist F-Secure ID PROTECTION?	2
Welche Systemvoraussetzungen müssen erfüllt sein?	2
Wie installiere ich F-Secure ID PROTECTION?	3
Kann ich von F-Secure KEY auf ID PROTECTION umsteigen?	6
Ich habe bereits ein My F-Secure Konto	6
Das Masterpasswort	7
Eine E-Mail-Adresse überwachen	10
Verwendung des Tresors	13
Automatisches Ausfüllen	20
Verbinden von Geräten	24
Sperrern der App	25
Sicherheit und Kryptographie	26
F-Secure ID PROTECTION deinstallieren	29

Sollte Ihnen dieses FAQ eine Frage nicht beantworten können, stehen wir Ihnen gerne persönlich zur Verfügung. Schreiben Sie uns eine E-Mail an hallo@edv-buchversand.de oder kontaktieren Sie uns telefonisch:

0 21 91 99 11 99

(Mo.-Fr.: 8:30 – 17:00 Uhr)

Was ist F-Secure ID PROTECTION?

F-Secure ID PROTECTION ist eine App, die verhindert, dass Sie Opfer von Identitätsdiebstahl werden.

Identitätsdiebstahl geschieht, wenn jemand die Identität oder personenbezogenen Daten einer anderen Person, wie Name, Personalausweisnummer, Kreditkartennummer oder Online-Anmeldeinformationen, ohne deren Erlaubnis verwendet, um ein Verbrechen oder einen Betrug zu begehen. Die Entdeckung von Identitätsdiebstahl ist nicht einfach. Sobald Informationen offen im Internet stehen, können sie dort jahrelang einsehbar bleiben.

Die Mehrzahl der Vorfälle von Identitätsdiebstahl geht von Cyberkriminellen aus, die schwache Passwörter der Benutzer ausnutzen.

F-Secure ID PROTECTION bietet Ihnen folgende Möglichkeiten:

- Sie schützen Ihre eigenen personenbezogenen Daten und die Ihrer Familie vor Cyberkriminalität.
- Sie erhalten Warnmeldungen und Hilfestellung zur Reaktion auf Vorfälle, wenn Ihre persönlichen Daten durch eine Datenpanne oder ein Daten-Leak öffentlich bekannt werden.
- Sie verbessern Ihre Sicherheit, indem Sie sichere und einzigartige Passwörter erstellen und diese auf allen Ihren Geräten synchronisieren.

Welche Funktionen sind enthalten?

- Passwortmanager
- Online-Identitätsüberwachung
- Datenpannenalarm

Welche Systemvoraussetzungen müssen erfüllt sein?

F-Secure ID PROTECTION ist für sowohl für mobile Geräte als auch für PCs und Mac-Computer verfügbar.

Installationsvoraussetzungen:

- Achten Sie darauf, dass Ihr Gerät die aufgeführten Systemanforderungen erfüllt.
- Sie benötigen eine aktive Internetverbindung, um Ihr Abonnement zu validieren und Updates zu erhalten.

Windows	Mac	Smartphone & Tablets
<ul style="list-style-type: none"> • Windows 10 • Windows 8.1 • Windows 7 (SP1) (ARM-basierte Tablets werden nicht unterstützt.)	<ul style="list-style-type: none"> • macOS 10.13 (High Sierra) und höher. 	<ul style="list-style-type: none"> • Android 6 und höher, iOS 13 und höher Weitere Informationen finden Sie bei Google Play oder im App Store .

Wie installiere ich F-Secure ID PROTECTION?

Dreh- und Angelpunkt für die Erstinstallation und die spätere Verwaltung Ihrer Lizenz ist Ihr persönlicher „My F-Secure Account“ unter my.f-secure.com. Hier weisen Sie Ihre Lizenz einzelnen Geräten zu und hier haben Sie auch jederzeit und von jedem Gerät Zugriff auf Ihr Abonnement.

My F-Secure Account erstellen

1. Loggen Sie sich mit Ihren Login-Daten in „*Mein Konto*“ bei edv-buchversand.de ein.
2. Unter „*Meine Software*“ finden Sie Ihre F-Secure Produkte einschließlich Ihrer neuen ID-PROTECTION Lizenz. Wenn Sie sich Ihre Lizenz ansehen, finden Sie Ihren Abonnement-Code und den Button „*Hier einlösen*“.
3. Mit „*Hier einlösen*“ werden Sie auf my.f-secure.com weitergeleitet, Ihr Abonnement-Code wird direkt übertragen und Sie können Ihren Account registrieren.
4. Nach der Registrierung erhalten Sie eine E-Mail mit einem Aktivierungslink. Nach Aktivierung ist Ihr My F-Secure Account erstellt.

Installation unter Windows

1. Um die App zu installieren, wählen Sie die Option „ID PROTECTION installieren“.
2. Wählen Sie die Option „*Mein Gerät*“ und anschließend „Weiter“.
3. Wählen Sie „Diesen Computer“ aus und wählen Sie „Download für Windows“.
4. Speichern Sie die heruntergeladene Datei, navigieren Sie zum **Download-Ordner**, und doppelklicken Sie auf die Datei, um die Installation zu starten.

Anmerkung: Wenn Sie dazu aufgefordert werden, geben Sie Ihre Administrator-Anmeldeinformationen ein, und wählen Sie „Ja“.

5. Wenn das Fenster **F-Secure ID PROTECTION – Einrichtung** angezeigt wird, lesen Sie die Endnutzer-Lizenzbestimmungen, und wählen Sie anschließend die Option „*Akzeptieren und fortfahren*“.
6. Wenn die Installation abgeschlossen ist, wählen Sie „*Los geht's*“.
7. Wenn das Fenster **Benennen Sie das neue Gerät** angezeigt wird, geben Sie den Namen des Geräts ein, und wählen Sie die Option Fortfahren.

Installation auf einem Mac

1. Um die App zu installieren, wählen Sie die Option „*ID PROTECTION installieren*“.
2. Wählen Sie die Option „*Mein Gerät*“ und anschließend „Weiter“.
3. Wählen Sie „Diesen Computer“ aus und wählen Sie „Download für Mac“.
4. Speichern Sie die heruntergeladene Datei, navigieren Sie zum **Download-Ordner** im Finder, und doppelklicken Sie auf die Datei, um die Installation zu starten.

Anmerkung: Wenn Sie dazu aufgefordert werden, geben Sie Ihre Administrator-Anmeldeinformationen ein, und wählen Sie „Ja“.

1. Wenn das Fenster **F-Secure ID PROTECTION – Einrichtung** angezeigt wird, lesen Sie die Endnutzer-Lizenzbestimmungen, und wählen Sie anschließend die Option „*Akzeptieren und fortfahren*“.
2. Wenn die Installation abgeschlossen ist, wählen Sie „*Los geht's*“.
3. Wenn das Fenster **Benennen Sie das neue Gerät** angezeigt wird, geben Sie den Namen des Geräts ein, und wählen Sie die Option „*Fortfahren*“.

Installation unter Android

1. Starten Sie Google Play, und suchen Sie nach F-Secure ID PROTECTION.
2. Wenn ID PROTECTION gefunden wurde, wählen Sie die Option „*Installieren*“.
3. Wählen Sie nach der erfolgreichen Installation von ID PROTECTION auf Ihrem Gerät die Option „*Öffnen*“.
4. ID PROTECTION wird geöffnet, und ein kurzes Tutorial über die Hauptfunktionen wird angezeigt.
5. Wischen Sie den Bildschirm nach links weiter, bis Sie zur letzten Seite gelangen, und wählen Sie „*Erste Schritte*“.
6. Die Seite Willkommen bei F-Secure ID PROTECTION wird geöffnet.
7. Lesen Sie die Endnutzer-Lizenzbestimmungen, und wählen Sie anschließend die Option „*Akzeptieren und fortfahren*“.
8. Gehen Sie folgendermaßen vor:
 - **Wenn Sie bereits ein Konto bei Ihrem Dienstanbieter haben**, geben Sie Ihre Anmeldeinformationen ein, und wählen Sie die Option „*Anmelden*“.
 - **Wenn Sie noch kein Konto haben**, registrieren Sie sich, und geben Sie dazu die nötigen Angaben (Vorname, Nachname und E-Mail-Adresse) ein, erstellen Sie ein sicheres Passwort, und wählen Sie abschließend die Option „*Akzeptieren und Konto erstellen*“.
9. Wenn das Fenster **Benennen Sie das neue Gerät** angezeigt wird, geben Sie den Namen des Geräts ein, und wählen Sie die Option „*Fortfahren*“.

Installation unter IOS

1. Starten Sie den Apple App Store, und suchen Sie nach **F-Secure ID PROTECTION**.
2. Laden Sie die App herunter und installieren Sie sie auf Ihrem Gerät.
3. Wählen Sie nach der erfolgreichen Installation von ID Protection auf Ihrem Gerät die Option „*Öffnen*“.
4. ID PROTECTION wird geöffnet, und ein kurzes Tutorial über die Hauptfunktionen wird angezeigt.
5. Wischen Sie den Bildschirm nach links weiter, bis Sie zur letzten Seite gelangen, und wählen Sie „*Erste Schritte*“.
6. Die Seite Willkommen bei F-Secure ID PROTECTION wird geöffnet.

7. Lesen Sie die Endnutzer-Lizenzbestimmungen, und wählen Sie anschließend die Option „*Akzeptieren und fortfahren*“.
8. Wenn das Fenster **Benennen Sie das neue Gerät** angezeigt wird, geben Sie den Namen des Geräts ein, und wählen Sie die Option „*Fortfahren*“.

Kann ich von F-Secure KEY auf ID PROTECTION umsteigen?

Ja! Die neue F-Secure App ID PROTECTION ersetzt jetzt in My F-Secure die App KEY als Teil des neuen Angebots zur Verhinderung von Identitätsdiebstahl. ID PROTECTION bietet nicht nur einen Passwortmanager, sondern auch eine Funktion zur E-Mail-Überwachung, um Datenpannen und andere Cyber-Sicherheitsvorfälle zu beobachten, die sich negativ auf Ihre Passwörter und persönlichen Daten auswirken können.

Bevor Sie den **Umstieg von F-Secure KEY auf ID PROTECTION** durchführen, exportieren Sie die vorhandenen Passwörter auf F-Secure KEY. Diese Funktion finden Sie unter den „*Einstellungen*“. Nach der Installation von ID PROTECTION werden die Passwörter einfach

Ich habe bereits ein My F-Secure Konto

[Ich habe ein Abonnement für SAFE. Kann ich dasselbe My F-Secure-Konto für ID PROTECTION verwenden?](#)

Nein! Dies ist aus technischen Gründen nicht möglich. Wenn Sie bereits ein My F-Secure-Konto für SAFE haben, ist dieses Konto nicht mit ID PROTECTION kompatibel.

Deshalb müssen Sie zwingend ein vollständig neues My F-Secure-Konto mit einer anderen E-Mail-Adresse einrichten. **Sie benötigen also zwei My F-Secure-Konten:** eines für SAFE und eines für ID PROTECTION.

TIPP: Beide Programme sind Bestandteil von F-Secure TOTAL. Gern erstellen wir Ihnen hier ein Angebot zum Umstieg auf das Gesamtpaket. Gern per Mail an hallo@edv-buchversand.de oder telefonisch unter **0 21 91 / 99 11 99**

Das Masterpasswort

Was ist das Masterpasswort von F-Secure ID PROTECTION?

Das Masterpasswort ist äußerst wichtig, da es Ihnen den Zugriff auf die App ermöglicht und der sichere Schlüssel zu Ihren Passwortdaten ist.

Sobald Sie F-Secure ID PROTECTION installiert und die Anwendung zum ersten Mal gestartet haben, werden Sie aufgefordert, ein Masterpasswort zu erstellen. Das Masterpasswort ist das einzige Passwort, das Sie sich merken müssen, nachdem Sie ID PROTECTION in Gebrauch genommen haben.

Beachten Sie die folgenden wichtigen Hinweise zum Masterpasswort

- Immer wenn Sie Ihr Masterpasswort ändern, müssen Sie einen neuen Wiederherstellungscode erstellen.
- Sie benötigen immer den aktuellen Wiederherstellungscode, um wieder Zugriff auf die App zu erhalten.
- Wenn Sie neue Geräte verbinden, fordert Sie die App möglicherweise dazu auf, einen neuen Wiederherstellungscode zu erstellen. Erstellen Sie in diesem Fall unbedingt einen neuen Wiederherstellungscode, da der alte seine Gültigkeit verliert.
- Wir empfehlen Ihnen, den Wiederherstellungscode als Bild zu speichern und dieses zur Aufbewahrung auszudrucken. Bewahren Sie den ausgedruckten Wiederherstellungscode unbedingt von Ihrem Gerät getrennt auf.

Masterpasswort vergessen?

Wählen Sie ein schwer zu erratendes Masterpasswort (oder eine Masterpassphrase), das Sie sich merken können, da Ihr Masterpasswort nicht mit der App zurückgesetzt werden kann, falls Sie es vergessen sollten. Dass ein vergessenes Masterpasswort nicht zurückgesetzt werden kann, ist eine bewusste Entscheidung von F-Secure, um Ihre Sicherheit und Privatsphäre zu stärken und Ihre Daten zu schützen.

Der **Wiederherstellungscode** bietet die einzige Möglichkeit, den Zugriff auf die Anwendung wiederzuerlangen, falls Sie das Masterpasswort vergessen haben sollten.

Warum gibt es keine Sicherheitsfrage zum Zurücksetzen des Masterpassworts?

Unsere Recherchen haben ergeben, dass es einfach ist, die richtigen Antworten auf typische Fragen zum Zurücksetzen von Passwörtern zu finden. Hinweis darauf geben öffentlich zugängliche Angaben über Sie oder Spuren, die Sie hinterlassen haben. Dazu gehören Daten wie Ihr Geburtsort, die Schule, die Sie besucht haben, der Name Ihres Lehrers, der Geburtsname Ihrer Mutter usw. Die Namen Ihrer Haustiere lassen sich über Feeds in sozialen Netzwerken ermitteln oder durch einfaches Befragen Dritter ohne Ihr Wissen.

Wichtig: Da Sicherheitsfragen Ihre Sicherheit beeinträchtigen, sind sie bei F-Secure ID PROTECTION nicht vorgesehen.

Erstellen eines Wiederherstellungscodes

F-Secure ID PROTECTION bietet Ihnen jedoch die Möglichkeit zum [Erstellen eines Wiederherstellungscodes](#) für Ihr Masterpasswort, sobald Sie die App in Gebrauch genommen haben. Der Wiederherstellungscodes stellt eine sichere Methode dar, Ihr Masterpasswort wiederzuerlangen, falls Sie es vergessen haben sollten.

Anmerkung: Wenn sich das Masterpasswort aus irgendeinem Grund ändert, müssen Sie einen neuen Wiederherstellungscodes erstellen, da alle alten Codes ihre Gültigkeit verlieren. Achten Sie deshalb darauf, dass der Wiederherstellungscodes stets aktuell und für Ihr aktuelles Masterpasswort gültig ist.

So erstellen Sie den Wiederherstellungscodes für das Masterpasswort

1. Öffnen Sie F-Secure ID PROTECTION.
2. Wählen Sie „*Einstellungen*“ → „*Wiederherstellungscodes erstellen*“.

Das Bild mit dem Wiederherstellungscodes wird automatisch erstellt.

3. Wählen Sie die Option „*Speichern*“, um das Bild zu speichern.
4. Wählen Sie einen Speicherort für die Datei aus und anschließend die Option „*Speichern*“.

5. Navigieren Sie zu dem Ordner, und drucken Sie das Bild mit dem Wiederherstellungscodes aus.

Anmerkung: Wir empfehlen Ihnen, den Code als Bild zu speichern und die Datei als Ausdruck aufzubewahren, anstatt sie in einem Cloud-Speicher abzulegen.

Verwenden des Wiederherstellungscodes zum Wiederherstellen eines vergessenen Masterpassworts

Wichtig: Sie können Ihr Masterpasswort nur wiederherstellen, wenn Sie zuvor einen Wiederherstellungscodes für das Masterpasswort erstellt haben.

So stellen Sie das Masterpasswort mit dem Wiederherstellungscodes wieder her

1. Öffnen Sie F-Secure ID PROTECTION.
2. Wählen Sie auf dem Anmeldebildschirm die Option „*Masterpasswort vergessen?*“.
3. Wählen Sie die Option „*Importieren*“.
4. Suchen und öffnen Sie die Bilddatei mit dem Wiederherstellungscodes, die Sie früher erstellt haben.

Ihr Masterpasswort wird auf dem Bildschirm angezeigt.

5. Wählen Sie „*Anmelden*“ aus.

Die Anwendung F-Secure ID PROTECTION wird geöffnet.

Ändern des Masterpassworts

1. Melden Sie sich bei der App an.
2. Wählen Sie „*Einstellungen*“ → „*Masterpasswort ändern*“.
3. Geben Sie Ihr aktuelles Masterpasswort ein.
4. Geben Sie das **neue Masterpasswort** ein.
5. Geben Sie das Masterpasswort erneut ein, und wählen Sie „*OK*“.

Ihr Masterpasswort wurde nun geändert. Wenn Sie das Masterpasswort auf einem Gerät ändern, müssen Sie das neue Masterpasswort auf allen verbundenen Geräten verwenden.

Wichtig: Wenn Sie zuvor einen Wiederherstellungscode für das Masterpasswort erstellt haben, müssen Sie für das neue Masterpasswort einen neuen Wiederherstellungscode erstellen. Mit dem Wiederherstellungscode für das Masterpasswort stellen Sie sicher, dass Sie das Masterpasswort wiederherstellen können, falls Sie es vergessen sollten.

Eine E-Mail-Adresse überwachen

Mit der Überwachung von F-Secure ID PROTECTION können Sie Ihre E-Mail-Adressen zur Überwachung hinzufügen und erhalten Hilfestellung, was zu tun ist, wenn Ihre persönlichen Daten von einer Datenpanne betroffen sind.

Die Benachrichtigungs-E-Mail enthält Informationen darüber,

- welche personenbezogenen Daten von der Datenpanne betroffen waren,
- worin die Panne bestand,
- welches Unternehmen oder welche Organisation betroffen war,
- wann die Datenpanne auftrat und welche weiteren personenbezogenen Daten mit der überwachten E-Mail-Adresse in Zusammenhang gebracht wurden, wie z. B. Passwörter, Kreditkartennummern, Hausanschrift usw.

Hinzufügen Ihrer ersten E-Mail-Adresse für die Überwachung

Sobald Sie das Produkt aktiviert und Ihr Masterpasswort erstellt haben, können Sie die erste E-Mail-Adresse zu den überwachten Elementen hinzufügen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie im linken Navigationsbereich die Option „*Überwachung*“ und anschließend „*Überwachung beginnen*“.

Wenn Sie nicht mit Ihrem My F-Secure-Konto angemeldet sind, geben Sie Ihre Anmeldeinformationen für My F-Secure ein. Dies ist unter Windows & Mac erforderlich. Unter IOS und Android werden die Adressen direkt in der App hinterlegt.

1. Wählen Sie die Option „+ *Überwachtes Element hinzufügen*“.
2. Geben Sie Ihre E-Mail-Adresse ein, und wählen Sie die Option „*Hinzufügen*“.

Wichtig: Wir haben eine E-Mail mit einem Bestätigungslink an Ihre E-Mail-Adresse geschickt.

3. Wählen Sie „OK“.

Die App überprüft sofort, ob Ihre E-Mail-Adresse von einer bekannten Datenpanne betroffen ist. Wenn Ihre E-Mail-Adresse im Zusammenhang mit einer bekannten Datenpanne auftaucht, werden diese Vorfälle in der Ansicht Überwachung aufgeführt.

Informationen über Ihre geleakten Daten

Um detailliertere Informationen über Ihre geleakten Daten und die empfohlenen Maßnahmen sehen zu können, müssen Sie zunächst Ihre E-Mail-Adresse bestätigen.

1. Öffnen Sie die **Bestätigungs-E-Mail**, und wählen Sie den Link, um zu bestätigen, dass dies Ihre E-Mail-Adresse ist

Diese E-Mail-Adresse wird automatisch zu Ihrer Kontakt-E-Mail-Adresse. Später können Sie diese in eine andere E-Mail-Adresse ändern.

2. Um Details zu Ihren öffentlich bekannt gewordenen Daten und Gegenmaßnahmen anzuzeigen, tippen Sie auf eine Datenpanne, die in der Ansicht Überwachung aufgeführt ist

Wichtig: Um das Risiko eines Missbrauchs Ihrer Daten auszuschließen, raten wir Ihnen, die empfohlenen Maßnahmen dringendst umzusetzen.

Hinzufügen weiterer Elemente zur Überwachung

So fügen Sie weitere Elemente zur Überwachung hinzu

1. Melden Sie sich bei Ihrem My F-Secure-Konto oder in der App an, und wählen Sie die Option „*ID PROTECTION-Überwachung*“
2. Wählen Sie die Option „*Überwachte Elemente*“
3. Wählen Sie die Option „*+ Überwachtes Element hinzufügen*“
4. Geben Sie in der Ansicht „*Neues überwachtes Element*“ Ihre E-Mail-Adresse ein, und wählen Sie die Option Hinzufügen

Wichtig: Wir haben eine E-Mail mit einem Bestätigungslink an Ihre E-Mail-Adresse geschickt.

5. Wählen Sie „OK“

Die App überprüft sofort, ob Ihre E-Mail-Adresse von einer bekannten Datenpanne betroffen ist. Wenn Ihre E-Mail-Adresse im Zusammenhang mit einer bekannten Datenpanne auftaucht, werden diese Vorfälle in der Ansicht Überwachung aufgeführt.

6. Öffnen Sie die **Bestätigungs-E-Mail**, und wählen Sie den Link, um zu bestätigen, dass dies Ihre E-Mail-Adresse ist

7. Um Details zu Ihren öffentlich bekannt gewordenen Daten und Gegenmaßnahmen anzuzeigen, tippen Sie auf eine Datenpanne, die in der Ansicht Überwachung aufgeführt ist

Wichtig: Um das Risiko eines Missbrauchs Ihrer Daten auszuschließen, raten wir Ihnen, die empfohlenen Maßnahmen dringendst umzusetzen.

Bearbeiten und Löschen von überwachten Elementen

Anmerkung: Sie können ein Element, das zur Überwachung hinzugefügt wurde, **nicht** direkt bearbeiten. Wenn Sie ein vorhandenes überwacht Element bearbeiten müssen, müssen Sie das Element zuerst löschen und dann erneut zur Überwachung hinzufügen.

So löschen Sie ein überwacht Element:

1. Melden Sie sich bei Ihrem My F-Secure-Konto oder in der App an, und wählen Sie die Option „ID PROTECTION-Überwachung“
2. Wählen Sie die Option „Überwachte Elemente“
3. Wählen Sie das Symbol mit den **drei Punkten** neben der zu löschenden E-Mail-Adresse und dann „Löschen“ → „Löschen“ aus

Das Element verschwindet aus der Liste der überwachten Elemente

Anmerkung: Um Ihre Kontakt-E-Mail-Adresse zu bearbeiten oder aus der Überwachung zu löschen, müssen Sie zunächst alle anderen E-Mail-Adressen löschen, falls vorhanden. Erst dann können Sie die Kontakt-E-Mail-Adresse bearbeiten oder löschen.

Verwendung des Tresors

Mit dem Tresor von F-Secure ID PROTECTION können Sie Passwort- und Zahlungskarteneinträge erstellen und bearbeiten, sichere Passwörter für Onlinedienste generieren und auf den Passwortverlauf zugreifen.

Welche Browser werden von F-Secure ID PROTECTION unterstützt?

Google Chrome	Microsoft Edge	Mozilla Firefox
---------------	----------------	-----------------

Merkmale eines guten Passworts

Die allgemeine Empfehlung für ein gutes Passwort lautet, dass es einzigartig sein sollte, eine Kombination aus Buchstaben, Zahlen und Sonderzeichen enthält und für Sie ebenso leicht zu merken wie es für andere schwer zu erraten ist.

Zusätzlich zu diesen allgemeinen Richtlinien gibt es noch einige weitere Maßnahmen, mit denen Sie die Sicherheit Ihrer Konten bei Onlinediensten verbessern können:

Nutzen Sie generierte Passwörter. Wenn Sie ein von F-Secure ID PROTECTION generiertes Passwort verwenden, gibt es kein Speichersystem oder sonstige Hinweise, mit denen das Passwort geknackt werden kann.

Ändern Sie Ihre Passwörter. Machen Sie es sich zur Gewohnheit, Ihre Passwörter von Zeit zu Zeit zu ändern. Sollte Ihnen dies zu schwerfallen, ändern Sie Ihr Passwort zumindest dann unbedingt sofort, wenn ein Dienst Sie auf eine potenzielle Datenpanne hinweist.

Verwenden Sie, wo immer es möglich ist, unterschiedliche E-Mail-Adressen für verschiedene Arten von Onlinediensten. Falls Ihr E-Mail-Konto gehackt wird, sind nicht gleich alle Ihre Online-Konten gefährdet.

Vermeiden Sie es möglichst, Ihre E-Mail-Adresse als Benutzernamen zu verwenden. Viele Dienste erstellen Konten automatisch mit Ihrer E-Mail-Adresse als Benutzernamen. Falls dies nicht erforderlich ist, verwenden Sie einen anderen Benutzernamen.

Warum Sie für jeden Dienst und jedes Konto ein eigenes Passwort verwenden sollten?

Sicherheitsexperten empfehlen im Allgemeinen die Verwendung sicherer, einzigartiger Passwörter für alle Ihre Onlinedienste und Konten.

Starke Passwörter, die mehrere verschiedene Arten von Zeichen enthalten, sind für einige Onlinedienste obligatorisch. Ein Passwort, das Sie bei der Registrierung eingeben, wird dann nicht akzeptiert, wenn es zu kurz oder nicht komplex genug ist.

Doch selbst wenn Sie sich ein hochkomplexes Passwort ausdenken, das für andere praktisch unmöglich zu erraten ist, ist die Sicherheit Ihres Kontos bei Onlinediensten gefährdet, wenn Sie für jedes Konto dasselbe Passwort verwenden. Wenn Hacker z. B. Zugang zu den Anmeldedaten für einen der von Ihnen genutzten Dienste erhalten, können sie diese Informationen verwenden, um auf alle Ihre anderen Online-Konten zuzugreifen, bei denen Sie dasselbe Passwort verwenden. Mit einem einzigartigen Passwort für jedes Konto erreichen Sie, dass im Falle einer Datenpanne bei einem der von Ihnen genutzten Dienste andere Konten nicht gefährdet sind.

Speichern eines neuen Passworts auf einem Mac oder PC

Sie können Ihre Passwörter sicher auf einem Desktopgerät speichern.

So speichern Sie ein neues Passwort

1. Öffnen Sie die App, und wählen Sie die Ansicht **Tresor** aus.
2. Wählen Sie die Option „+ Neu hinzufügen“ → „Passwort“.

Die Seite **Neu hinzufügen** wird geöffnet.

3. Geben Sie im Feld **Titel** den Namen der Website oder des Onlinediensts ein.
4. Wählen Sie das **Globussymbol** neben dem Feld **Titel** und anschließend eine Farbe sowie ein Symbol für den Eintrag. Wählen Sie abschließend „OK“.
5. Geben Sie im Feld **Benutzername** den Benutzernamen ein, den Sie für die Website oder den Dienst verwenden.
6. Führen Sie im Feld **Passwort** eine der folgenden Aktionen aus:
 - Erstellen Sie ein starkes Passwort oder eine Passphrase.

- Lassen Sie die App über das Würfelsymbol ein starkes, zufälliges Passwort für Sie generieren.

Wenn Sie mit dem Passwort zufrieden sind, wählen Sie die Option „*Fertig*“.

Anmerkung: Wählen Sie das Symbol mit dem geöffneten Auge, wenn Sie das Passwort anzeigen möchten.

7. Geben Sie in das Feld **Webadresse** die Webadresse (URL) der Anmeldeseite dieses Onlinediensts ein.
8. Im Feld **Notizen** können Sie jegliche weitere Informationen festhalten.
9. Wählen Sie die Option „*Hinzufügen*“.

Die neuen Anmeldeinformationen wurden nun der App hinzugefügt.

Wichtig: Wenn Sie ein Passwort in F-Secure ID PROTECTION ändern oder generieren, denken Sie daran, Ihr Passwort auch im Webdienst oder in der App zu ändern.

Speichern eines neuen Passworts auf einem Mobilgerät

Sie können neue Passwörter in der App auf Ihrem Mobilgerät speichern.

So speichern Sie ein neues Passwort

1. Öffnen Sie die App, und wählen Sie die Ansicht **Tresor** aus.
2. Wählen Sie das **Plus-Symbol**.
3. Wählen Sie die Option „*Passwort*“.
4. Geben Sie in dem Feld **Titel** einen beschreibenden Namen für den Eintrag ein.
5. Wählen Sie das **Stiftsymbol** über dem Titel, um die Hintergrundfarbe und ein Symbol für den Eintrag auszuwählen. Wenn Sie fertig sind, bestätigen Sie Ihre Auswahl, indem Sie die Option „*Fertig*“ wählen.
6. Geben Sie im Feld **Benutzername** den Benutzernamen ein, den Sie für die App oder die Website verwenden.
7. Führen Sie im Feld **Passwort** eine der folgenden Aktionen aus:
 - Erstellen Sie ein starkes Passwort oder eine Passphrase.
 - Lassen Sie die App über das Würfelsymbol ein starkes, zufälliges Passwort für Sie generieren.

Wenn Sie mit dem Passwort zufrieden sind, wählen Sie die Option „*Fertig*“.

Anmerkung: Wählen Sie das Symbol mit dem geschlossenen Auge, um Ihr Passwort auszublenden.

8. Geben Sie in das Feld **Webadresse** die Webadresse (URL) der Anmeldeseite dieser Website ein.
9. Im Feld **Notizen** können Sie jegliche weitere Informationen festhalten.
10. Um den Eintrag zu sichern, wählen Sie die Option „*Fertig*“.

Die neuen Anmeldeinformationen wurden nun der App hinzugefügt.

Wichtig: Wenn Sie ein Passwort in F-Secure ID PROTECTION ändern oder generieren, denken Sie daran, das Passwort auch im Webdienst oder in der jeweiligen App zu ändern.

Schrittweise Anweisungen zum Bearbeiten von Einträgen in der App.

Wenn Sie einen Eintrag erstellt haben, können Sie ihn später bei Bedarf bearbeiten.

So bearbeiten Sie einen vorhandenen Eintrag

1. Öffnen Sie die App, und wählen Sie die Ansicht Tresor aus
2. Wählen Sie den Eintrag aus, den Sie bearbeiten möchten
3. Wählen Sie das Stiftsymbol, um die Ansicht Bearbeiten zu öffnen
4. Nehmen Sie die gewünschten Änderungen vor
5. Wählen Sie Speichern, um die Änderungen zu sichern

Löschen eines Eintrags aus dem Tresor

Nicht mehr benötigte Einträge können Sie löschen.

So löschen Sie einen Eintrag

1. Öffnen Sie die App, und wählen Sie die Ansicht **Tresor** aus
2. Wählen Sie den Eintrag aus, den Sie löschen möchten
3. Wählen Sie das **Stiftsymbol**, um die Ansicht **Bearbeiten** zu öffnen
4. Um den Eintrag zu löschen, wählen Sie die Option „*Entfernen*“

5. Um das Löschen zu bestätigen, wählen Sie die Option „OK“ im Dialogfeld Eintrag entfernen

Ändern eines Passworts mit der App

Wenn Sie ein Passwort ändern müssen, kann die App ein sicheres Passwort für Sie generieren.

Sie können die Länge und die Komplexität des Passworts wählen.

So ändern Sie ein Passwort

1. Öffnen Sie die App, und wählen Sie die Ansicht **Tresor** aus.
2. Rufen Sie den Eintrag auf, dessen Passwort Sie ändern möchten, und wählen Sie das **Stiftsymbol**.
3. Wählen Sie im Feld **Passwort** das **Würfel-Symbol**.
4. In der Ansicht **Passwort generieren** können Sie Folgendes tun:
 - Ziehen Sie den Schieberegler von einer Seite zur anderen, um die gewünschte Zeichenanzahl für Ihr Passwort auszuwählen.
 - Wählen Sie die Art der Zeichen (Klein- und Großbuchstaben, Zahlen und Sonderzeichen), die Sie in Ihrem Passwort verwenden möchten.
 - Wählen Sie die Option „Generieren“, um das generierte Passwort zu ändern.
5. Um das generierte Passwort zu nutzen, wählen Sie die Option „Verwenden“.
6. Um den Eintrag zu sichern, wählen Sie die Option „Speichern“.

Wichtig: Wenn Sie ein Passwort in ID PROTECTION ändern oder generieren, denken Sie daran, das Passwort auch im Webdienst oder in der jeweiligen App zu ändern.

Zugreifen auf den Passwortverlauf

Das Passwortverlaufsprotokoll enthält möglicherweise vorhandene frühere Passwörter für den jeweiligen Onlinedienst.

Nachdem Sie ein Passwort in der App geändert haben, müssen Sie sich bei dem Onlinedienst möglicherweise noch mit dem bisherigen Passwort anmelden. Häufig müssen

Sie auch das bisherige Passwort eingeben, um das Passwort für einen Dienst ändern können.

So greifen Sie auf die früheren Passwörter zu

1. Öffnen Sie die App, und wählen Sie die Ansicht **Tresor** aus.
2. Öffnen Sie den Eintrag, dessen frühere Passwörter Sie einsehen möchten.
3. Wählen Sie das Symbol für den **Passwortverlauf (Uhr)**.

Anmerkung: Wenn das Symbol nicht angezeigt wird, sind keine früheren Passwörter für diesen Onlinedienst vorhanden.

Die Ansicht Passwortverlauf wird geöffnet.

4. Um die ausgeblendeten Passwörter anzuzeigen, markieren Sie das Kontrollkästchen in der Spalte Anzeigen.

Anmerkung: Sie können den Passwortverlauf löschen, indem Sie die Schaltfläche Löschen wählen.

5. Um die Ansicht Passwortverlauf zu schließen, wählen Sie die Schaltfläche „**Schließen**“.

Importieren und Exportieren von Passwörtern

Mit F-Secure ID PROTECTION können Sie Ihre Tresordaten aus der App exportieren und Passwörter aus anderen Passwortmanagern in die App importieren.

Anmerkung: Das Importieren und Exportieren der Passwortdaten ist nur mit den Produktversionen für Windows und Mac möglich.

Importieren von Passwörtern aus anderen Passwortmanagern

Sie können Ihre Daten aus F-Secure ID PROTECTION oder anderen Passwortmanagern importieren, die den Export in ein offenes Textformat unterstützen. Der Import ist nur mit den Versionen für Windows und Mac möglich.

F-Secure ID PROTECTION unterstützt den Import von Passwörtern aus folgenden Passwortmanagern:

- Dashlane
- F-Secure ID PROTECTION
- Google Chrome
- KeePassX V2
- LastPass

So importieren Sie Passwörter in F-Secure ID PROTECTION

1. Öffnen Sie **F-Secure ID PROTECTION**.
2. Wählen Sie „*Einstellungen*“ → „*Passwörter importieren*“.
3. Wählen Sie über die Dropdownliste den Passwortmanager aus, von dem Sie Passwörter importieren möchten.

Es werden Anweisungen zum Export Ihrer Passwörter für den ausgewählten Passwortmanager angezeigt.

4. Wenn Sie die Datei exportiert und lokal gespeichert haben, ziehen Sie sie per Drag & Drop zu ID PROTECTION.

F-Secure ID PROTECTION importiert die Passwörter automatisch und meldet Ihnen, wie viele Passwörter importiert wurden.

Exportieren von Tresordaten aus der App

Sie können Ihre Daten aus F-Secure ID PROTECTION exportieren. Der Export ist nur mit den Versionen für Windows und Mac möglich.

So exportieren Sie Ihre Tresordaten aus der App

1. Öffnen Sie **F-Secure ID PROTECTION**.
2. Wählen Sie „*Einstellungen*“ → „*Passwörter exportieren*“.
3. Wählen Sie die Option „*In meinen Tresor exportieren*“.

Das Fenster Masterpasswort wird geöffnet.

4. Geben Sie das Masterpasswort ein, und klicken Sie auf „*OK*“.
5. Wählen Sie einen Speicherort für die Datei aus und anschließend die Option „*Speichern*“.

Standardmäßig werden die Passwortdaten in der Datei ExportedPasswords.fsk (F-Secure ID PROTECTION-Austauschdatei) am angegebenen Ort gespeichert.

Anmerkung: Wenn Sie Ihre Daten aus dem Tresor exportieren, wird die Datei im Klartext exportiert und kann daher leicht von anderen gelesen werden. Speichern Sie diese Datei daher an einem Ort, wo sie nicht leicht zugänglich ist oder beschädigt werden könnte. Denken Sie auch daran, die Datei zu löschen, nachdem Sie die Daten übertragen haben.

Automatisches Ausfüllen

Mit der Funktion zum automatischen Ausfüllen von F-Secure ID PROTECTION können Sie sich bei Apps und Websites anmelden, ohne Benutzernamen und Passwörter manuell eingeben zu müssen.

Sie müssen den Benutzernamen, das Passwort und die Webadresse eines Dienstes in F-Secure ID PROTECTION hinterlegen, damit das automatische Ausfüllen funktioniert. Wenn Ihre Anmeldeinformationen in F-Secure ID PROTECTION gespeichert sind, können Sie die App Ihren Benutzernamen und Ihr Passwort in einer App oder auf einer Website automatisch eintragen lassen.

Automatisches Ausfüllen auf Desktopgeräten

Sie können die App Ihre Anmeldeinformationen automatisch ausfüllen lassen.

Mit ID PROTECTION können Sie schnell auf Onlinedienste zugreifen. Verwenden Sie dazu die Funktion zum automatischen Ausfüllen auf der Anmeldeseite des jeweiligen Diensts.

Installieren und Autorisieren der Browsererweiterung zum automatischen Ausfüllen

Um Ihre Benutzernamen und Passwörter in Chrome, Edge oder Firefox automatisch einzutragen, müssen Sie die Funktion zum automatischen Ausfüllen im Browser in den Einstellungen aktivieren und die Browsererweiterung oder das Add-on in Ihrem Browser installieren.

So installieren und autorisieren Sie die Browsererweiterung

1. Öffnen Sie **F-Secure ID PROTECTION**.
2. Navigieren Sie zu „*Einstellungen*“ → „*Allgemeine Einstellungen*“
3. Wählen Sie unter **Automatisch ausfüllen** die Option „*Automatisches Ausfüllen im Browser aktivieren*“, und gehen Sie wie folgt vor:

• In Chrome und Edge:

1. Suchen Sie im [Chrome Web Store](#) nach „*Password Manager by F-Secure*“ und wählen Sie „*Hinzufügen*“ aus

Hinweis: Auch Edge-User nutzen den Chrome Web Store

2. Wählen Sie in dem sich öffnenden Fenster die Option „*Erweiterung hinzufügen*“
3. Die Erweiterung **Password Manager by F-Secure** wird dem Browser hinzugefügt, und das Symbol des Passwortmanagers wird in der oberen rechten Ecke des Browsers angezeigt. Jetzt müssen Sie die Erweiterung autorisieren
4. Kehren Sie zur **App** zurück, und wählen Sie unter „*Einstellungen*“ unten auf der Seite die Option „*In Zwischenablage kopieren*“, um den Autorisierungscode zu kopieren, der zum Abschließen der Einrichtung benötigt wird
5. Wählen Sie im Browser das Symbol „*Passwordmanager von F-Secure*“ in der oberen rechten Ecke des Browsers, und fügen Sie den kopierten Autorisierungscode ein
6. Wählen Sie die Option „*Autorisieren*“ → „*Schließen*“. Die Browsererweiterung ist jetzt aktiviert

• In Firefox:

1. Öffnen Sie [Firefox Browser ADD-ONS](#) und suchen Sie nach „*Password Manager von F-Secure*“ und wählen Sie die Option „*Zu Firefox hinzufügen*“ → „*Hinzufügen*“ aus
2. Die Erweiterung wird dem Browser hinzugefügt, und das Symbol des Passwortmanagers F-Secure KEY wird in der oberen rechten Ecke des Browsers angezeigt. Bestätigen Sie dies mit „*OK*“. Jetzt müssen Sie die Erweiterung autorisieren
3. Kehren Sie zur **App** zurück, und wählen Sie unter „*Einstellungen*“ unten auf der Seite die Option „*In Zwischenablage kopieren*“, um den Autorisierungscode zu kopieren, der zum Abschließen der Einrichtung benötigt wird

4. Wählen Sie im Browser das Symbol „*Passwortmanager von F-Secure*“ in der oberen rechten Ecke des Browsers, und fügen Sie den kopierten Autorisierungscode ein
4. Wählen Sie die Option „*Autorisieren*“ → „*Schließen*“. Das Symbol ändert sich in das Symbol F-Secure ID PROTECTION, und die Browsererweiterung ist jetzt aktiviert

Automatisches Ausfüllen für den Zugriff auf Onlinedienste

Sie können schnell auf Onlinedienste zugreifen, ohne Ihre Anmeldeinformationen manuell eingeben zu müssen.

So greifen Sie auf den Onlinedienst zu

1. Melden Sie sich mit Ihrem Masterpasswort bei F-Secure ID PROTECTION an
2. Suchen Sie im Tresor den Onlinedienst, auf den Sie zugreifen möchten, und klicken Sie auf das Symbol für den Eintrag

Die Anmeldeseite des Dienstes wird in Ihrem Standardbrowser geöffnet.

Anmerkung: Falls sie sich nicht öffnen lässt, stellen Sie sicher, dass Sie die korrekte Webadresse der Anmeldeseite für den Eintrag im Tresor eingegeben haben.

3. Wählen Sie im Feld **Benutzername** das Symbol für ID PROTECTION und anschließend den Dienst aus der Dropdownliste aus. Die App trägt Ihren Benutzernamen und Ihr Passwort ein

Anmerkung: Wenn das Symbol im Feld **Benutzername** nicht angezeigt wird, zeigen Sie die Dropdownliste der verfügbaren Onlinedienste mit der Tastenkombination Strg + Alt + V an.

Automatisches Ausfüllen unter iOS einschalten

Mit der Funktion zum automatischen Ausfüllen können Sie sich bei Apps und Websites anmelden, ohne Benutzernamen und Passwörter manuell eingeben zu müssen.

Sie müssen den Benutzernamen, das Passwort und die Webadresse eines Dienstes in F-Secure ID PROTECTION hinterlegen, damit das automatische Ausfüllen funktioniert. Wenn Ihre Anmeldeinformationen in F-Secure ID PROTECTION gespeichert sind, können Sie die App Ihren Benutzernamen und Ihr Passwort in einer App oder auf einer Website automatisch eintragen lassen.

So aktivieren Sie die Funktion zum automatischen Ausfüllen auf Ihrem iPhone oder iPad

1. Navigieren Sie auf Ihrem Gerät zu „*Einstellungen*“ → „*Passwörter & Accounts*“
2. Wählen Sie unter **Passwörter & Accounts** die Option „*Automatisch ausfüllen*“
3. Schalten Sie unter **Automatisch ausfüllen** die Option „*Automatisch ausfüllen*“ ein, falls sie ausgeschaltet ist
4. Wählen Sie unter **Ausfüllen zulassen von**, die Option „*ID PROTECTION*“

Die Funktion zum automatischen Ausfüllen ist auf Ihrem Gerät jetzt einsatzbereit.

Anmelden bei einer App oder Website unter iOS

Damit F-Secure ID PROTECTION den korrekten Eintrag für eine App oder Website anzeigen kann, müssen Sie die URL im entsprechenden Eintrag angegeben haben.

So melden Sie sich bei einer App oder Website auf Ihrem iPhone oder iPad an

1. Öffnen Sie die Anmeldeseite der App oder der Website, und tippen Sie auf das Feld **Benutzername**.

Passwörter werden oben auf der Tastatur Ihres Geräts angezeigt.

2. Wählen Sie die Option „*Passwörter*“
3. Wählen Sie die Option „*ID PROTECTION*“
4. Entsperren Sie die App
5. Wählen Sie den gewünschten Eintrag aus

ID PROTECTION füllt die Anmeldeinformationen des Diensts für Sie aus.

6. Wählen Sie „*Anmelden*“ aus

Jetzt sind Sie bei der App oder dem Webdienst angemeldet.

Anmelden bei einer App oder Website unter Android

Damit F-Secure ID PROTECTION den korrekten Eintrag für eine App oder Website anzeigen kann, müssen Sie die URL im entsprechenden Eintrag angegeben haben.

So melden Sie sich bei einer App oder Website auf Ihrem Android-Gerät an

1. Öffnen Sie die Anmeldeseite der App oder der Website.
2. Tippen Sie auf das Feld **Benutzername**, und wählen Sie den Eintrag zum automatischen Ausfüllen aus dem Dropdownmenü aus.

Anmerkung: Wenn F-Secure ID PROTECTION gesperrt ist, entsperren Sie die App mit Ihrem Fingerabdruck oder dem Masterpasswort.

3. Wählen Sie den gewünschten Eintrag aus.

ID PROTECTION füllt die Anmeldeinformationen des Diensts für Sie aus. Jetzt sind Sie bei der App oder dem Webdienst angemeldet.

Verbinden von Geräten

Sie können Ihre Geräte verbinden, um Ihre Tresordaten geräteübergreifend zu synchronisieren.

Damit Sie Ihre Tresordaten geräteübergreifend synchronisieren können, müssen Sie die Geräte verbinden, auf denen F-Secure ID PROTECTION installiert ist.

Wenn die App entweder nur auf einem Mobilgerät oder nur auf Ihrem Computer installiert ist, werden Ihre Tresordaten nur auf diesem Gerät gesichert. Die App ist so gestaltet, dass Ihre Daten jederzeit auf allen verbundenen Geräten immer aktuell zur Verfügung stehen. Wenn Sie Ihre Daten auch auf einem anderen Gerät haben, müssen sich keine Sorgen darüber machen, wenn Ihr Gerät verloren geht, gestohlen oder beschädigt wird. Denn Ihre Daten bleiben auf Ihren anderen Geräten unbeschadet verfügbar.

Warnung: Wenn Sie die App nur auf einem Mobilgerät nutzen und dieses auf Werkseinstellungen zurücksetzen, werden dadurch auch alle Ihre Tresordaten von dem Gerät gelöscht. Danach gibt es keine Möglichkeit mehr, an diese Daten zu gelangen.

Synchronisieren Ihrer Tresordaten mit anderen Geräten

Sie können Ihre Tresordaten mit Ihren anderen Geräten synchronisieren, auf denen die App installiert ist.

So synchronisieren Sie Ihre Daten

1. Öffnen Sie F-Secure ID PROTECTION.
2. Wählen Sie die Option „*Geräte verbinden*“.

Es wird automatisch ein Synchronisierungscode generiert, der jeweils 60 Sekunden lang gültig ist. Unmittelbar nach dem Ablauf der Gültigkeit des aktuellen Codes wird ein neuer Code generiert.

3. Öffnen Sie die App auf dem Gerät, auf dem Sie Ihre App-Daten synchronisieren möchten.
4. Je nachdem, ob es sich bei dem anderen Gerät um ein Mobilgerät oder ein Desktopgerät handelt, gehen Sie wie folgt vor:
 - Navigieren Sie auf einem Mobilgerät zu „*Menü*“ → „*Geräte verbinden*“, und geben Sie den in Schritt 2 erzeugten Synchronisierungscode ein.
 - Wählen Sie auf einem Desktopgerät die Option „*Geräte verbinden*“, und geben Sie den in Schritt 2 erzeugten Synchronisierungscode ein.
5. Wählen Sie die Option „*Verbinden*“.
6. Wenn Sie dazu aufgefordert werden, geben Sie Ihr Masterpasswort ein, das Sie auf dem Gerät verwenden, mit dem Sie den Synchronisierungscode generiert haben.
7. Wenn die Synchronisierung erfolgreich abgeschlossen ist, wählen Sie die Option „*Bestätigen*“.

Ihre Daten sind jetzt zwischen diesen beiden Geräten synchronisiert. Wenn Sie weitere Geräte verbinden möchten, wiederholen Sie die obigen Schritte für jedes Gerät. Beachten Sie, dass Sie den Synchronisierungscode auf jedem verbundenen Gerät generieren können.

Sperren der App

Wir empfehlen Ihnen, die App immer zu sperren, wenn Sie sie nicht verwenden.

Entsperren und Sperren der App

Wenn Sie die App nicht verwenden, empfehlen wir Ihnen, sie zu sperren, um eine zusätzliche Sicherheitsschicht hinzuzufügen.

Gehen Sie wie folgt vor, um die App zu entsperren bzw. zu sperren:

- Um die App zu entsperren, geben Sie Ihr Masterpasswort ein, und wählen Sie die Option „*Entsperren*“.
- Um die App zu sperren, wählen Sie im linken Navigationsbereich die Option „Sperren“.

Anmerkung: Standardmäßig wird die App nach fünf Minuten automatisch gesperrt. In den Einstellungen können Sie den Zeitraum einstellen, nach dem die App gesperrt wird: 5 Minuten, 15 Minuten, 30 Minuten, 60 Minuten, 10 Stunden und eine Woche.

Sicherheit und Kryptographie

In diesem Abschnitt werden die Hauptprinzipien der Gestaltung von F-Secure ID PROTECTION erläutert und wie dadurch die Anonymität unserer Benutzer sowie deren sensible Daten zu respektiert und geschützt werden.

So sichert die App Daten mit doppelter Verschlüsselung

Unter diesem Thema wird erläutert, wie wir Ihre Daten mit mehreren Verschlüsselungsschichten sichern.

Die Verschlüsselung und Entschlüsselung der in der App gespeicherten Daten erfolgt ausschließlich auf Ihrem eigenen Gerät. Jedes Mal, wenn Sie das Masterpasswort für ID PROTECTION eingeben, fügt es eine zusätzliche Verschlüsselungsebene hinzu, indem es

einen Verschlüsselungsschlüssel generiert, mit dem Ihre verschlüsselten Daten in ID PROTECTION entschlüsselt werden. Dies geschieht unter Verwendung des PBKDF2-Standards (Password-Based Key Derivation Function 2), der dem Passwort einen Salt-Wert (Zufallsdaten) hinzufügt und aus den resultierenden Daten mit der HMAC-SHA256-Funktion einen Hash erstellt. Dieser Vorgang wird 20.000 Mal wiederholt.

Das Masterpasswort und der Master-Verschlüsselungsschlüssel werden niemals gespeichert. Die Verschlüsselungsschlüssel existieren nur während der aktiven Nutzung des Produkts. Wenn Sie den F-Secure ID PROTECTION ausschalten, wird der Verschlüsselungsschlüssel zerstört. Wir haben keine Möglichkeit, Informationen, die Sie in F-Secure ID PROTECTION gespeichert haben, zu entschlüsseln.

Dieses Sicherheitsniveau bedeutet jedoch gleichzeitig, dass F-Secure keine Möglichkeit hat, Ihr Passwort oder Ihre Daten für Sie wiederherzustellen, falls Sie das Masterpasswort vergessen sollten. Darüber hinaus trackt F-Secure Sie nicht, wenn Sie Ihre Daten geräteübergreifend synchronisieren.

So wird die Passwortstärke berechnet

Unter diesem Thema wird erläutert, wie die Passwortstärke berechnet wird.

Die Berechnung der Passwortstärke in F-Secure ID PROTECTION basiert auf der Entropie eines Passworts.

Die Passwortentropie gibt an, wie einfach es für eine Software zum Knacken von Passwörtern ist, ein Passwort vorherzusagen. Je mehr Passwörter die Software ausprobieren muss, bevor sie das Passwort erraten kann, desto höher ist seine Entropie.

Um den maximalen Entropiewert zu erhalten, ist es wichtig, mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen (oder Symbol) in dem Passwort zu verwenden. Vermeiden Sie auch sämtliche Zeichenfolgen wie „12345678“ oder „abcdefgh“, und verwenden Sie keine Zeichenwiederholungen (z. B. „aaaaaaaa“). Vermeiden Sie die Verwendung häufiger männlicher oder weiblicher Namen, häufiger Wörter und typischer Passwörter. Zuletzt hat auch die Passwortlänge einen Einfluss auf die Passwortentropie.

Werden die Inhalte aller Eingabefelder in ID PROTECTION verschlüsselt?

Ja, die Inhalte aller Eingabefelder werden verschlüsselt, bevor die Daten gespeichert werden.

Sind meine Informationen während der Übertragung zwischen ID PROTECTION und dem Server jederzeit verschlüsselt?

Ja, sie sind immer verschlüsselt. Wir verwenden TLS/SSL, um Ihre Informationen während der gesamten Datenübertragung zu sichern.

So bewahren wir die Anonymität in der App

Für uns besteht keine Möglichkeit zur Entschlüsselung der Daten, die Sie in der App gespeichert haben.

Jeder Nutzer von F-Secure ID PROTECTION bleibt für F-Secure anonym. Deshalb können wir die Daten einzelner Benutzer nicht identifizieren. Wir haben zu keinem Zeitpunkt Einblick in Ihre Daten und können sie daher weder entschlüsseln noch an Dritte weitergeben.

Dieses Datenschutzniveau erreichen wir durch den im Produkt eingesetzten Advanced Encryption Standard (AES) mit 256-Bit-Blockverschlüsselung. Zusätzlich setzen wir als Betriebsmodus für unsere Blockchiffren den CCM-Modus (Counter with CBC-MAC) ein. Hierbei handelt es sich um einen authentifizierten Verschlüsselungsalgorithmus, der sowohl Authentifizierung als auch Vertraulichkeit gewährleistet.

Sowohl die Wahl der Verschlüsselungsmethode als auch der Schutz der Anonymität der Benutzer waren bewusste Entscheidungen, um die Sicherheit des Produkts zu verbessern und die Privatsphäre unserer Kunden zu schützen.

Die F-Secure ID PROTECTION-Server sind Eigentum von F-Secure und werden von F-Secure innerhalb der Europäischen Union in Übereinstimmung mit finnischem Recht und unter Einhaltung der EU-Vorschriften betrieben.

Erfasst F-Secure Informationen über die URLs und andere Daten, die Benutzer in ID PROTECTION eingeben?

Nein. F-Secure erfasst keinerlei personenbezogene Daten oder Informationen, die Sie in F-Secure ID PROTECTION eingeben.

F-Secure ID PROTECTION deinstallieren

Wie kann ich F-Secure ID PROTECTION vollständig von einem PC entfernen?

Befolgen Sie diese Anweisungen, wenn Sie die App vollständig von Ihrem Windows-Computer entfernen möchten.

Um das Produkt vollständig von Ihrem Computer zu entfernen, müssen Sie sowohl die App F-Secure ID PROTECTION als auch den lokalen Speicher (mit Ihren Tresordaten) einzeln entfernen.

Anmerkung: Bevor Sie mit dem Entfernen der App beginnen, stellen Sie sicher, dass sie nicht mehr läuft.

So entfernen Sie das Produkt von Ihrem Computer

1. Navigieren Sie zu „Systemsteuerung“ „Programm deinstallieren“
2. Wählen Sie F-Secure „ID PROTECTION“ → „Deinstallieren“. Dadurch wird die App von Ihrem Computer entfernt