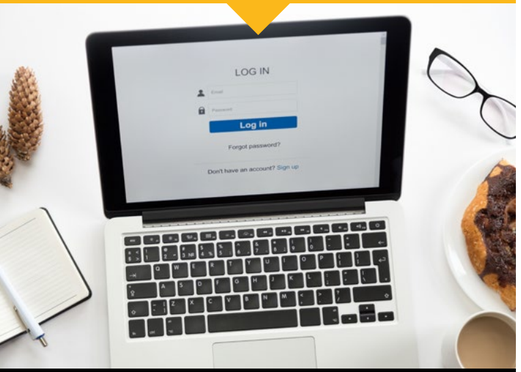
Comment quelqu'un peut-il découvrir mon mot de passe ?



Il a essayé toutes les combinaisons possibles.

Il connaît un autre de mes mots de passe.

Il m'a amené à dévoiler mon mot de passe.

J'ai saisi mon mot de passe sur un faux site web/une fausse appli.

J'ai partagé mon mot de passe avec quelqu'un.

Un mot de passe sécurisé en 4 étapes :

ÉTAPE 1 : Unique et difficile à deviner

Commencez par une phrase qui vous plaît et qui est facile à mémoriser, sans informations personnelles.

Par ex.: **Tous les midis, deux licornes et cinq flamands roses dansent sur l'arc en ciel !**

ÉTAPE 2 : Utilisez au moins 12 caractères

Utilisez uniquement les premières lettres des mots de votre phrase.

Par ex.: **T**ous **l**es **m**idis, **d**eux **l**icornes **e**t **c**inq **f**lamands **r**oses **d**ansent **s**ur **l**'arc **e**n **c**iel !

T l m , d l e c f r d s l ' a e c !

ÉTAPE 3 : Ajoutez des éléments à votre phrase

Utilisez des majuscules/minuscules **(Aa)** et remplacez certaines lettres par des chiffres **(3, 5, 9 ...)** et des caractères spéciaux **(!?.+')**.

deux = 2 cinq = 5 e = €

Par ex.:

T l m , 2 l € 5 f r d s l ' a € c !

ÉTAPE 4 : N'utilisez jamais le même mot de passe pour plusieurs sites web/applis

Vous pouvez utiliser les lettres du nom/logo du site web/de l'appli et p.ex. les intégrer à la deuxième ou à l'avant-dernière position de votre mot de passe.

Par ex.: **Facebook = FB**

FB + T l m , 2 l € 5 f r d s l ' a € c ! =

T F l m , 2 l € 5 f r d s l ' a € c B !

Alternative :

Utilisez une phrase complète « phrase de passe »

Check-list

- [ ] **Utilisez des mots de passe sûrs !**
- [ ] **Gardez votre mot de passe secret !**
- [ ] **Ne partagez pas votre mot de passe !**
- [ ] **Utilisez un autre mot de passe pour chaque site web ou application !**
- [ ] **Activez l'authentification à deux facteurs si elle est proposée.**

- **Authentification à deux facteurs :** ***www.silversurfer.lu/2facteurs***
- **Testez votre mot de passe :** ***pwdtest.bee-secure.lu***
- **Avez-vous déjà été piraté ?** ***haveibeenpwnd.com***
- **Utilisez un gestionnaire de mots de passe** (programme pour sauvegarder les mots de passe) **par ex.: KeePass**

Pour plus d'information:

www.silversurfer.lu
www.bee-secure.lu

Internet en sécurité
Les règles d'or

1 Cliquer malin
Les escroqueries en ligne peuvent être coûteuses. Restez vigilant et prenez votre temps. En cas de doute, mieux vaut ne pas cliquer.

2 Utiliser des mots de passe forts
Un mot de passe contient au moins 12 caractères et est composé de chiffres, de lettres majuscules et minuscules, ainsi que de caractères spéciaux. Utilisez un mot de passe différent pour chaque sites ou applications.

3 Protéger l'identité
Plus les informations que vous divulguez sur Internet sont personnelles, plus elles sont attrayantes, voire lucratives pour les cybercriminels. Ainsi, ne donnez que le minimum d'informations lorsque celles-ci ne sont pas nécessaires.

4 Faire des mises à jour régulières
Les mises à jour consistent à corriger les lacunes de sécurité dans les programmes. Assurez-vous que les logiciels et les extensions soient actualisés.

5 Protéger l'ordinateur
Un logiciel anti-virus et un pare-feu activé sont absolument essentiels.

6 Sauvegarder les données
Pour éviter de perdre vos fichiers et données en cas d'incident, des sauvegardes doivent être effectuées régulièrement.

Tirage: 1000 exemplaires
Hackdorf Flyer v.2 - 05/2019

Sicheres Passwort

BEE SECURE silversurfer.lu

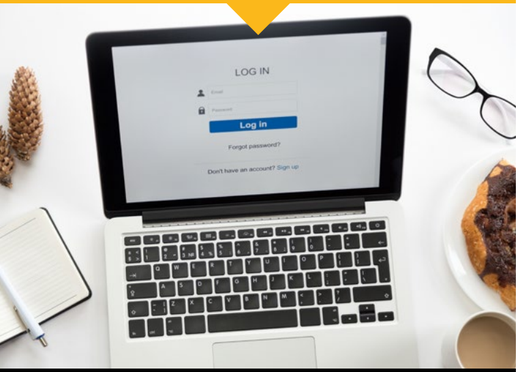
CENTER FIR ALTERSFROEN

SENIOREN SECHERHEETS BERODER

Co-financed by the European Union
Connecting Europe Facility

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Famille, de l'Intégration et à la Grande Région

Wie konnte jemand mein Passwort herausfinden?



Jemand hat alle möglichen Kombinationen ausprobiert.

Jemand kennt ein anderes meiner Passwörter.

Jemand hat mich dazu gebracht mein Passwort zu verraten.

Ich habe mein Passwort auf einer gefälschten Webseite/App eingegeben.

Ich habe mit jemandem mein Passwort geteilt.

In 4 Schritten zu Ihrem sicheren Passwort:

1. SCHRITT: Einzigartig und schwer zu erraten

Beginnen Sie mit einem Satz der Ihnen gefällt und den Sie sich gut merken können ohne persönliche Informationen.

Beispiel: **Mein Passwort mache ich mit einem Satz und hüte es wie einen Schatz!**

2. SCHRITT: Mindestens 12 Zeichen sollten es schon sein

Benutzen Sie nur die Anfangsbuchstaben der Wörter aus Ihrem Satz.

Beispiel: **M**ein **P**asswort **m**ache **i**ch **m**it **e**inem **S**atz **u**nd **h**üte **e**s **w**ie **e**inen **S**chatz!

M P m i m e S u h e w e S !

3. SCHRITT: Schmücken Sie Ihren Satz aus

Nutzen Sie Groß-/Kleinbuchstaben **(Aa)** und ersetzen Sie bestimmte Buchstaben durch Zahlen **(1, 2, 3...)** und Sonderzeichen **(!?.+')**.

einem = 1 S = 5 e = €

M P m i m 1 5 u h € w € 5 !

4. SCHRITT: Verwenden Sie nie das gleiche Passwort für mehrere Webseiten/Apps

Was Sie machen können ist die Buchstaben vom Namen/Logo der Webseite/App her ableiten und diese dann z. B. an zweiter und zweitletzter Stelle in Ihr Passwort einbauen.

Beispiel: **Facebook = FB**

FB + M P m i m 1 5 u h € w € 5 ! =

M F P m i m 1 5 u h € w € 5 B !

Alternative :

Verwenden Sie einen vollständigen Satz "Pass-Satz"

Checkliste

- [ ] **Benutzen Sie sichere Passwörter!**
- [ ] **Halten Sie Ihr Passwort geheim!**
- [ ] **Teilen Sie Ihr Passwort mit niemandem!**
- [ ] **Benutzen Sie für jedes Konto ein anderes Passwort**
- [ ] **Aktivieren Sie die 2-Faktor-Authentifizierung, wenn verfügbar!**

- **2-Faktor-Authentifizierung:** ***www.silversurfer.lu/2facteurs***
- **Testen Sie Ihr Passwort:** ***pwdtest.bee-secure.lu***
- **Sind Sie schon mal gehackt worden?** ***haveibeenpwnd.com***
- **Wollen Sie Ihre Passwörter speichern?** Benutzen Sie einen ***Passwort-Manager*** (Programm zur Passwortverwaltung) **bspw. KeePass**

Weitere Informationen:

www.silversurfer.lu
www.bee-secure.lu

Sicher im Netz – Die goldenen Regeln

1 Clever klicken
Online-Betrug kann teuer werden. Bleiben Sie wachsam und lassen Sie sich Zeit. Im Zweifelsfall besser nicht anklicken.

2 Starke Passwörter benutzen
Ein starkes Passwort ist mindestens 12 Zeichen lang und besteht aus Zahlen, großen und kleinen Buchstaben sowie Sonderzeichen. Für verschiedene Zwecke sollten verschiedene Passwörter benutzt werden.

3 Identität schützen
Je mehr persönliche Daten Sie im Internet preisgeben, um so attraktiver und ggf. auch lukrativer werden Sie für Cyberkriminelle. Geben Sie also nur die nötigsten Informationen preis, falls erforderlich.

4 Regelmäßig Programme aktualisieren
Updates schließen Sicherheitslücken in Programmen. Vergewissern Sie sich, dass alle Programme und „Plugins" immer auf dem letzten Stand sind.

5 Den Computer schützen
Ein Anti-Virus Programm und eine aktivierte Firewall sind unbedingt erforderlich.

6 Daten sichern
Damit im Ernstfall keine Daten verloren gehen, sollten regelmäßig Sicherungskopien gemacht werden.

Notice légale

Cette publication a été réalisée par le SNJ (Service National de la Jeunesse) dans le cadre du projet BEE SECURE.

Tirage: 1000 exemplaires
Hackdorf Flyer v.2 - 05/2019

Mot de passe sécurisé

BEE SECURE silversurfer.lu

CENTER FIR ALTERSFROEN

SENIOREN SECHERHEETS BERODER

Co-financed by the European Union
Connecting Europe Facility

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Famille, de l'Intégration et à la Grande Région