Communiqué de presse

Journée internationale du changement des mots de passe 2023. La sécurité des mots de passe reconsidérée

Aix-la-Chapelle, Allemagne, 31 janvier 2023 – Chaque année, le 1er février, la Journée internationale de changement des mots de passe est censée nous rappeler à quel point nos mots de passe sont importants pour notre sécurité. Cette année, il y a de bonnes nouvelles pour ceux d'entre nous qui trouvent les nombreuses règles de création de mots de passe fastidieuses : trouver des mots de passe sécurisés ne nécessite aucun effort.

Les sujets de ce communiqué de presse :

- **L'exemple à ne pas suivre : les mots de passe les plus populaires en 2022**
- **Important : utiliser des mots de passe différents**
- **La prise de notes est autorisée**
- **Authentification à deux facteurs (2FA)**
- **Le garant de la sécurité de votre réseau Wi-Fi**
- **Prix et disponibilité**

Communiqué de presse

L’exemple à ne pas suivre : les mots de passe les plus populaires en 2022

Tout d'abord, une mauvaise nouvelle pour les fainéants : les mots de passe doivent répondre à un niveau minimum de sécurité, et donc de complexité. Trop souvent, ce n'était pas le cas l'année dernière, comme l'a montré par exemple l'Institut Hasso-Plattner. Cet institut informatique évalue chaque année les mots de passe les plus utilisés en Allemagne et, comme les années précédentes, il est arrivé à une conclusion qui donne à réfléchir pour 2023. La première place est occupée par la combinaison simple de chiffres "123456", qui devance la deuxième version la plus fréquente, légèrement plus avancée, "123456789". Les dix meilleurs mots de passe allemands de 2022 montrent sans aucun doute une marge d’amélioration considérable.

Mais il y a aussi de bonnes nouvelles pour ceux qui sont agacés par ce qui est souvent défini comme une norme de sécurité : les mots de passe sécurisés n’ont pas besoin de 20 caractères et n’ont pas besoin d’être modifiés mensuellement. De nombreuses règles de mot de passe bien connues sont maintenant considérées comme obsolètes. C’est principalement parce qu’ils sont difficilement réalisables dans les applications quotidiennes.

Important : utiliser des mots de passe différents

Aujourd’hui, l’internaute lambda doit mémoriser un nombre considérable de mots de passe. Nous nous connectons quotidiennement pour accéder à nos comptes bancaires, aux sites de e-commerces, aux réseaux sociaux et aux services de streaming. Notre vie devient de plus en plus numérique, et par conséquent, les mots de passe envahissent nos vies. Il est irréaliste de s’attendre à ce que quelqu’un mémorise des mots de passe multiples, divers et longs, qui doivent être changés régulièrement, sans quelque chose pour nous aider à les retenir. Théoriquement, la mémorisation serait la méthode la plus sûre, mais elle échoue dans la pratique. Même l’Office fédéral allemand de la sécurité de l’information (BSI) l’a reconnu et a supprimé plusieurs conseils traditionnels et bien intentionnés dans ses dernières recommandations pour la communication concernant la sécurité des mots de passe.

Le plus important de nos jours est d’utiliser différents mots de passe pour différents comptes. La raison est facile à comprendre: c’est déjà assez grave si un mot de passe tombe entre de mauvaises mains. Et les dommages peuvent être rapidement minimisés si, par exemple, les intrus n’ont qu’un bref accès à un service de streaming. En revanche, si la combinaison volée d'une adresse électronique et d'un mot de passe ouvre tout le coffre-fort numérique d'une personne, les dommages peuvent devenir considérables. En isolant les données d'accès individuelles, un changement de mot de passe n'est vraiment nécessaire que si le service en question a subi une violation de données.

À leur tour, et en fonction de l’importance d’un compte, les mots de passe individuels peuvent être un peu moins complexes, mais certainement pas aussi simples que « 123456789 ». La question qui se pose naturellement est de savoir comment se souvenir de tant de mots de passe différents.

La prise de notes est autorisée

Cela peut sembler fou, mais cela est désormais logique : selon le BSI, l'écriture des mots de passe, qui a été fortement déconseillée pendant des années, « ne devrait pas être présentée comme négative en soi ». Il y a un hic, cependant. Les mots de passe notés doivent être stockés correctement ; de telle sorte qu'ils ne puissent pas être trouvés facilement par n'importe qui. Les post-it avec les identifiants d'accès à vos comptes bancaires en ligne et affichés sur le bord de votre écran sont encore tabous. En revanche, des copies stockées en toute sécurité des informations de connexion les plus importantes peuvent renforcer la sécurité en ligne si elles encouragent l'utilisation de mots de passe de haute qualité.

La gestion des mots de passe sécurisés est encore plus pratique avec un gestionnaire de mot de passe, mais selon le BSI, beaucoup de gens sont encore sceptiques à leur sujet. Ces outils stockent les mots de passe, n'oublient rien et peuvent même être utilisés pour générer des mots de passe aléatoires. Ensuite, vous pouvez utiliser des applications appropriées pour les appareils mobiles ou des extensions pour les navigateurs Web pour rendre la saisie des mots de passe encore plus pratique. Ces derniers temps, un large éventail d'outils de ce type a vu le jour. Chaque gestionnaire de mots de passe propose de nombreuses fonctionnalités. L'identification de vos besoins et faiblesses vous permettra de choisir l'outil le plus adapté. Que ce soit en version payante ou gratuite, pour la mémorisation ou pour la génération de mots de passes complexes et uniques, vous aurez l'embarras du choix : NordPass, Roboform, Bitwarden ou encore Dashlane.

Authentification à deux facteurs

L'utilisation de « l'authentification à deux facteurs », souvent aussi appelée vérification en deux étapes, est fortement recommandée. Cela garantit que, lors de la connexion avec un nom de connexion et un mot de passe, un deuxième composant de vérification est ajouté pour confirmer l'identité de l'utilisateur. Les moyens courants de le faire incluent les e-mails avec des liens de confirmation et les messages SMS avec des codes à usage unique. La plupart d'entre nous se sont habitués à ce type de connexion via nos banques. Mais de plus en plus de fournisseurs d'autres services proposent également une authentification à deux facteurs en option. Lorsqu'elle est disponible, l'authentification à deux facteurs doit toujours être activée. Elle garantit que même les comptes avec des mots de passe plus faibles soient bien protégés. Par exemple, pour accéder à votre compte, un tiers aurait besoin non seulement de vos données de connexion, mais également d'un accès à votre téléphone.

Le garant de la sécurité de votre réseau Wi-Fi

Il est particulièrement important de penser au mot de passe pour votre Wi-Fi privé. Après tout, cette clé d'accès protège votre réseau Wifi domestique et tous les appareils qui y sont connectés. Par conséquent, vous devez faire attention non seulement à définir un mot de passe sécurisé, mais aussi à bénéficier des fonctions de sécurité de pointe. Il s'agit, par exemple, d'un cryptage basé sur les normes actuelles (au moins WPA2). Ces exigences doivent être non seulement satisfaites non seulement au niveau du routeur Internet, mais aussi de tous les autres appareils transportant le signal Internet à travers les quatre murs de votre maison, tels que les répéteurs Wi-Fi. Les spécialistes allemands des réseaux de devolo à Aix-la-Chapelle assurent une extension sécurisée du réseau avec la série de produits devolo Magic WiFi. Les adaptateurs polyvalents transforment n'importe quelle prise de courant en un point d'accès ultra-rapide avec ou sans fil et répondent aux normes

de sécurité les plus avancées : WPA3 et WPA2. Avec cryptage 128 bits, ils sécurisent le réseau domestique contre les intrus. Des options intelligentes telles que l'accès invité par code QR ou application permettent aux utilisateurs de donner à leurs invités des mots de passe à la fois complexes et sécurisés tout en garantissant un accès pratique.

Prix et disponibilité

Le moyen idéal pour commencer à utiliser des réseaux domestiques sécurisés avec devolo est le Starter Kit devolo Magic 1 WiFi mini avec deux adaptateurs au prix de 99,90 euros. Les utilisateurs plus avancés qui optent pour le kit de démarrage devolo Magic 2 WiFi next pour 199,90 euros bénéficient d'une forte combinaison de Wi-Fi et de Gigabit LAN. Avec le kit de démarrage devolo Magic 2 WiFi 6 au prix de 239,90 euros, vous pouvez créer un réseau Wi-Fi maillé moderne entre vos quatre murs.
Tous les prix spécifiés incluent la TVA. Tous les produits mentionnés ci-dessus sont compatibles entre eux afin que le réseau domestique puisse être étendu de manière flexible. De plus, devolo fournit à tous les produits une garantie du fabricant de trois ans.

Contact presse

HOP'*N* WORLD

Nathalie LESNE
N° de téléphone : +33 665 15 64 37
Adresse e-mail : nathalie@hopnworld.com

David BONNIVARD
N° de téléphone : +33 6 29 43 91 83
Adresse e-mail : david@hopnworld.com

Ce texte et les images actuelles des produits peuvent également être consultés à l'adresse www.devolo.fr dans la section médias du site Web de devolo.

À propos de devolo

devolo développe des solutions de réseaux domestiques intelligents qui envoient l'Internet haut débit dans tous les coins de votre maison ou de votre appartement. Notre produit phare est devolo Magic, une technologie qui permet d'établir des réseaux intelligents et flexibles à partir de câbles électriques existants. La gamme de produits est complétée par des systèmes Wi-Fi maillés innovants et des solutions pour les connexions en fibre optique. Avec plus de 45 millions d'adaptateurs CPL vendus, devolo fait partie des leaders du marché mondial. Plus de 800 évaluations et distinctions internationales en tant que meilleurs produits soulignent notre leadership en matière d'innovation. devolo a été fondée en 2002 à Aix-la-Chapelle, en Allemagne, et est représentée dans plus de 10 pays.