MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

LA LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

n° 3/2025

LA THEMATIQUE DU MOIS:
Les mots de passe

INTRODUCTION

Le mot de passe, c'est un peu comme une clé qui vous permet d'accéder à un espace particulier (site de vente, logiciel professionnel, réseau social etc...)..
Mais auriez-vous l'idée de n'avoir qu'une seule et même clé pour entrer dans votre maison, votre bureau ou dans le bar du coin ? Non ? Alors, pourquoi le faire avec votre mot de passe dans ce cas ?
Et s'il est assez facile de reconnaître dans un trousseau quelle clé ouvre une porte déterminée, c'est un peu plus compliqué pour les mots de passe...comment alors retenir des mots de passe différents ?

Pourquoi un mot de passe ?

Le mot de passe est une clé d'accès à un espace numérique (ou même physique dans le cas d'un code pour un coffre-fort ou encore le code d'une porte d'entrée d'immeuble). Tout le monde en est convaincu, c'est important, c'est personnel, ça ne doit pas être communiqué etc... mais alors pourquoi ne pas utiliser son mot de passe comme on utilise une clé physique ?
Par exemple, laisseriez-vous votre trousseau de clés sur la table d'un lieu public sans surveillance ? Mettriez-vous votre clé dans une boîte aux lettres que vous ne connaissez pas parce quelqu'un vous a dit « vas-y, je surveille ta maison pendant les vacances, laisse-la, ne t'inquiète pas, c'est ma spécialité» ?
C'est pourtant bien ce que l'on fait lorsqu'on enregistre ses mots de passes dans son navigateur ou lorsque on rentre un mot de passe sur une page qui nous a été indiquée par un lien envoyé par mail.

Qu'est ce qu'un « bon » mot de passe ?

Un bon mot de passe, c'est un mot de passe que personne ne connaît, totalement personnel, et qui est assez robuste pour que personne ne puisse le deviner sans notre accord. Les spécialistes s'accordent pour considérer qu'un bon mot de passe contient plus de 12 caractères avec des minuscules, des majuscules, des chiffres, et des caractères spéciaux. Dans les faits, plus le mot de passe est long et plus ses caractères sont diversifiés, plus il sera difficile à « craquer » et donc meilleur il sera.

D'accord, mais en plus il faut en avoir plusieurs ??

OUI ! Avoir un bon mot de passe ne veut pas dire qu'il ne sera jamais découvert. Admettons que vous ayez le même mot de passe sur Facebook qu'au travail. Si Facebook se fait voler ses mots de passe, alors celui qui les achète a potentiellement aussi votre mot de passe pour accéder aux données de votre entreprise ou de votre commune... Avoir un mot de passe par service ou par site permet de limiter les risques en cas de compromission d'un seul d'entre eux. Perdre un compte Facebook ce n'est pas très grave, mais perdre un compte Facebook et être à l'origine d'une fuite de données sensibles au sein de votre entreprise, c'est autre chose...

Mais alors comment les retenir ?

Il existe heureusement des outils à télécharger ou en ligne pour vous aider : des gestionnaires de mots de passe ou encore des coffres-forts de mots de passe. En voici les principales caractéristiques :

GESTIONNAIRE DE MOTS DE PASSE :

Vos données sont accessibles depuis tous vos appareils, n'importe où et n'importe quand.
Vous pouvez synchroniser votre coffre-fort de mots de passe sur plusieurs appareils en même temps.
Même si elles sont chiffrées, les données sont stockées ailleurs.
Vous avez besoin d'une connexion Internet pour accéder à vos mots de passe.

COFFRE-FORT DE MOTS DE PASSE :

Aucune connexion Internet n'est nécessaire,
Il élimine totalement le risque que quelqu'un viole votre coffre-fort à moins que votre appareil ne soit saisi.
Vous ne pouvez accéder à votre coffre-fort que depuis un seul appareil, ce qui en limite l'utilisation,
Si vous perdez l'appareil ou s'il est cassé ou détruit d'une manière ou d'une autre, vous pouvez perdre toutes vos données.

Le coffre-fort est bien plus sécurisé que le gestionnaire. Si ce dernier est bien plus pratique et chiffre les mots de passe, ceux-ci sont en fait en possession d'un service tiers. Si ses serveurs sont détruits ou se font attaquer, vous pouvez perdre vos mots de passe.

Et avec tout ça, il faut rajouter une double authentification (2FA)?!

La double authentification est une couche de sécurité supplémentaire qui permet de confirmer votre action et d'éviter les clics trop rapides, et qui s'assure aussi que vous êtes bien la personne détentrice du mot de passe. Sans elle, un malfrat qui aurait découvert votre mot de passe pourrait l'utiliser sans problème. A l'inverse, si vous utilisez la double authentification, non seulement vous vous prémunissez de toute utilisation frauduleuse de votre mot de passe, mais en plus vous pourrez faire le nécessaire car vous saurez qu'il est corrompu et qu'il est temps de le changer. Car oui, il faut déjà considérer que les avancées technologiques permettront un jour de contourner cette 2FA....

CONCLUSION

Nous entendons tous les jours des recommandations et des rappels sur les mots de passe. Et pourtant, tous les jours, ce sont aussi des milliers de comptes qui sont bloqués ou compromis.
En dépit tous ces outils que nous venons de vous présenter, il faut bien être conscient qu'il n'existe pas de solution parfaite. Même la 2FA peut être contournée par un escroc qui vous met en confiance et vous convainc de lui communiquer le code de sécurité ou de valider votre face id au moment voulu. Aussi, **soyez vigilants** et **cloisonnez vos informations**, même avec un mot de passe de 64 caractères associé à un verrouillage biométrique !

+ D'INFOS

ANJ AUTORITÉ NATIONALE DES JEUX

Grand Est Cybersécurité — CENTRE D'ASSISTANCE DE PROXIMITÉ — 0 970 512 525

CYBER MALVEILLANCE .GOUV.FR

PHAROS — PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-Enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est

Directeur de la publication: GCA O.KIM
Responsable éditorial: COL L. GRAU
Rédacteur: ADJ M.KNOBLOCH

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
Laurent.grau@gendarmerie.interieur.gouv.fr
Mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie: