La sécurité informatique passe par un bon mot de passe

La politique de changement des mots de passe du Groupe ESEO évolue et cela peut perturber certains d'entre vous. Afin de vous accompagner le mieux possible vous trouverez ci-après quelques conseils et bonnes pratiques afin de comprendre d'une part les raisons d'une telle évolution et d'autres parts des conseils afin d'assurer cette transition de la façon la plus douce

Pourquoi changer son mot de passe ?

Vous vous connectez à tous vos services numériques grâce à ce couple identifiant et mot de passe uniques. Il est donc important que ce mot de passe réponde à des normes de sécurité suffisantes pour protéger vos outils et éviter les intrusions dans vos données.
Par défaut, vous avez choisi votre mot de passe ou l'avez modifié mais celui-ci ne répond à aucune éxigence de complexité. Il ne présente donc plus de garantie de confidentialité suffisante.

Penser à changer régulièrement son mot de passe

Les mots de passe peuvent circulent en clair sur les réseaux. Des techniques malveillantes simples (sniffers, espions, chevaux de Troie…), peuvent être mises en œuvre sur les réseaux pour capter celui-ci à l'insu des utilisateurs. C'est pourquoi, même robuste, un mot de passe doit être modifié régulièrement et ce tous les 180 jours désormais.

Veiller à la confidentialité de son mot de passe

Vous ne devez communiquer votre mot de passe à personne, sous aucun prétexte, tant à l'oral qu'à l'écrit. Ne le saisissez que lorque vous êtes certain de l'authenticité de l'emetteur de la demande.
Méfiez-vous particulièrement des messages électroniques frauduleux qui vous incitent à taper votre mot de passe sous prétexte de vouloir mettre à jour votre boîte à lettre électronique.
Sur vos navigateurs internet nous vous déconseillons fortement la mémorisastion des mots de passe pour des raisons évidentes.
Bien entendu banissez post-it ou autre document sur lequel serait écrit votre mot de passe.

Comment bien changer mon mot de passe ?

Un mot de passe fort est un mot de passe qui est difficile à retrouver, même à l'aide d'outils automatisés. La force d'un mot de passe dépend de plusieurs critères. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules. Un mot de passe ne doit pas pouvoir être trouvé dans un dictionnaire par exemple ni pouvoir être déduit de vos éléments personnels (nom du chien, prénom des enfants, date de naissance, …). Il aura au minimum 12 caractères.
L'agence nationale pour la sécurité informatique préconise deux méthodes pour définir des mots de passe robustes faciles à mémoriser.

La méthode pue consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir.
Par exemple, la phrase :
"j'ai acheté huit CD pour cent euros"

deviendra

ght8CD%€

• La méthode des premières lettres consiste à garder les premières lettres d'une phrase (citation, paroles de chanson,...) en veillant à ne pas utiliser que des minuscules.
Par exemple la citation :
"un tiens vaut mieux que deux tu l'auras"
deviendra
1TvmQ2tl@