académie
Versailles

RÉGION ACADÉMIQUE
ÎLE-DE-FRANCE

MINISTÈRE
DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Versailles, le 11 janvier 2017

Le Recteur de l'Académie de Versailles
Chancelier des Universités

A

Mesdames et Messieurs les personnels
de l'Académie de Versailles

Rectorat
3, boulevard
de Lesseps
78017
Versailles
Cedex

Dossier suivi par

Jacky GALICHER
Directeur des Systèmes
d'Information

Tél. :
01 30 83 48 00
Mél
ce.dsi@ac-versailles.fr

Objet : Mesures de cyber sécurité en vigueur dans le contexte actuel.

Le renforcement de la posture VIGIPIRATE, de la cyber sécurité, ainsi que la nécessité d'accroître la vigilance qui correspond à une posture permanente de sécurité me conduisent à rappeler certaines bonnes pratiques d'usage du numérique.

Vous trouverez des bonnes pratiques et des informations utiles, pour vos usages numériques professionnels et personnels, dans le document « conseils aux usagers » qui est publié sur le site www.gouvernement.fr, à l'adresse suivante : http://www.gouvernement.fr/risques/conseils-aux-usagers.

Parmi ces bonnes pratiques, j'attire plus particulièrement votre attention sur celles qui sont décrites ci-dessous à propos de l'ouverture des courriels, la séparation des usages entre moyens informatiques personnels et professionnels, le choix de vos mots de passe, la saisie de la chaine d'alerte de sécurité des systèmes d'information (SSI).

Lorsque vous recevez des courriels, prenez les précautions suivantes avant de les ouvrir :

- l'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message,
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts,
- si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer,
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire),
- ne suivez pas les liens figurant dans un message électronique. En cas de nécessité d'accès, privilégiez la navigation directe sur le site Internet référencé,
- n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

Séparer vos usages professionnels de vos usages personnels :

- Utilisez la messagerie académique pour tous vos usages professionnels,
- Ne transférez pas les messages professionnels vers une messagerie personnelle,
- Utilisez les services fournis ou recommandés par l'académie avant d'envisager de partager et de stocker vos documents professionnels sur un espace de stockage public (informatique en nuage).

Choisissez des mots de passe robustes :

- composés d'au moins 8 caractères :
  - mélangeant majuscules, minuscules, chiffres et caractères spéciaux,
  - n'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance,
  - ne formant pas de mots figurant dans le dictionnaire.

Pièce jointe: règles et conseils pour les mots de passe.

En pratique, vous disposez de 2 méthodes simples pour définir un mot de passe :

- la méthode phonétique : "J'ai acheté 5 CD pour cent euros cet après-midi" : ght5CD%E7am,
- la méthode des premières lettres : "Un tiens vaut mieux que deux tu l'auras" : 1tvmQ2tl'A.

Quelques recommandations supplémentaires pour vos mots de passe :

- n'utilisez pas le même mot de passe pour tout, notamment pour accéder à votre banque en ligne et votre messagerie personnelle ou professionnelle,
- méfiez-vous des logiciels qui vous proposent de stocker vos mots de passe.

Vous trouverez des règles et conseils complémentaires, en cliquant sur le lien suivant, puis en renseignant le mot de passe MdP16*Pv :
https://edu-nuage.ac-versailles.fr/index.php/s/7AmqIG5F7iPQCb0

Par ailleurs une chaîne d'alerte de sécurité des systèmes d'information (SSI) de l'académie a été mise en place pour signaler :

- un courriel de hameçonnage ou de rançongiciel (logiciel de rançon),
- une usurpation de votre identité,
- la défiguration d'un site web professionnel ou de l'académie.

Pour déclarer un incident de sécurité et assurer son suivi en préservant les règles de confidentialité, il convient de saisir un ticket d'incident dans CARIINA (depuis le portail ARENA, domaine « Support et Assistance ») en utilisant la rubrique « sécurité » ou par courriel, en cas d'urgence, à : alerte-ssi@ac-versailles.fr.

La chaîne d'alerte de sécurité des systèmes d'information fonctionne de la manière suivante :

- au sein des EPLE (établissements publics locaux d'enseignement) :
  - les personnels informent le chef d'établissement des incidents constatés,
  - le chef d'établissement déclare l'incident conformément au dispositif préalablement cité et informe le DASEN.
- au sein des écoles :
  - les personnels informent le directeur d'école des incidents constatés,
  - le directeur d'école déclare l'incident conformément au dispositif préalablement cité et informe l'IEN (Inspecteur de circonscription),
  - l'IEN ou un conseiller TICE peut également déclarer l'incident conformément au dispositif préalablement cité.
- au sein des services académiques :
  - les personnels informent le chef de service des incidents constatés,
  - le chef de service déclare l'incident.

Je compte sur le renforcement de votre vigilance lors des usages numériques. Si nécessaire, vous pouvez solliciter la mission TICE de votre Direction des services départementaux de l'éducation nationale (DSDEN), la Délégation académique au numérique éducatif (DANE) ou la Direction des systèmes d'information (DSI) pour vous conseiller et vous assister.

Daniel FILATRE

académie Versailles

REGLES ET CONSEILS POUR LES MOTS DE PASSE

Sécurité
12/10/2012

Dans le cadre de l'utilisation d'outils informatiques mis à votre disposition (poste de travail, messagerie, ...), il vous est généralement demandé de choisir des mots de passe afin de sécuriser les accès à ces outils. Il est de la première importance de sélectionner un mot de passe « solide » et de respecter certaines règles. Par mot de passe « solide », nous entendons un mot de passe qu'un programme informatique ne pourra pas trouver ni une personne persévérante deviner.

Règles de base

- Elaborer un mot de passe de **8 caractères minimum** (pas de lettre accentuée, pas d'espace)
- Utiliser pour élaborer ce mot de passe des caractères différents :
  - avec au moins 1 majuscule,
  - avec au moins 1 minuscule,
  - avec au moins 1 chiffre,
  - avec au moins 1 caractère spécial choisi parmi les caractères suivants & " ' (- _) = $ * *,(la virgule)* ; : ! + % ? *.(le point)* / # { [| \ @] } < >
- Mémoriser le mot de passe : si ce n'est pas possible, le stocker en lieu sûr.
- Eviter d'enregistrer le mot de passe dans le client de messagerie, le navigateur, ...lorsque c'est proposé
- Ne jamais dévoiler votre mot de passe à qui que ce soit[1] et ne jamais l'envoyer par courriel
- Choisir un mot de passe fondamentalement différent à chaque renouvellement

Comment choisir son mot de passe et s'en souvenir

Un bon mot de passe est un mot de passe sûr, qui sera donc **difficile à retrouver** même à l'aide d'outils automatisés **mais facile à retenir**.

Pour ce faire, il existe des moyens mnémotechniques pour fabriquer et retenir des mots de passe sûrs.

1. **Méthode phonétique**

Cette méthode 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 cet après-midi »* deviendra **« ght8CD%E7am ».**

2. **Méthode des premières lettres**

Cette méthode 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 »** donnera **«1tvmQ2tl'A ».**

Ne pas utiliser

- Toute chaîne de caractères correspondante à un mot ou prénom simple

Ex: Annie25@, 41%Porte, Maison1%, 3Versailles! sont à éviter car facilement attaquables avec certains logiciels

- De chaînes séquentielles du clavier ex : azer....., ni de nombres qui se suivent ex : 1234....., ni plusieurs fois les mêmes caractères ex : bbb@B333
- Ne pas utiliser d'informations personnelles (nom, prénom, date de naissance, code postal, etc.), que ce soient les vôtres ou celles d'un proche.

[1] Sauf exception (exemple : boîtes fonctionnelles partagées) : voir charte TIC académique p 4

Rédacteur : Direction des systèmes d'information de l'académie de Versailles