MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE
Liberté
Égalité
Fraternité

Secrétariat général

Service de défense et de sécurité (SDS)
Sécurité des systèmes d'information
Affaire suivie par : **Nicolas Eslous**
Mél. : fssi@education.gouv.fr

Direction du numérique pour l'éducation (DNE)
Affaire suivie par : **Dominique Alglave**
Mél. : rssi-education@education.gouv.fr

N° 2024-1018

Paris, le 3 avril 2024,

Le Secrétaire général,
haut fonctionnaire de défense et de sécurité

à

Mesdames et messieurs les recteurs
de région académique,

Mesdames et messieurs les recteurs d'académie,

Mesdames et messieurs les vice-recteurs

Objet : Actualisation des règles de gestion des mots de passe d'accès aux services numériques

Les cas d'usurpations d'identité numériques vont croissant (cf. les nombreux courriels frauduleux envoyés depuis des boites de messagerie du ministère ou la vague actuelle de messages frauduleux dans les ENT) et augmentent les risques de cybersécurité (vols de données, rançongiciels...).

Ces fraudes s'appuient sur le mauvais comportement de certains utilisateurs (qui se font piéger en installant à leur insu des logiciels malveillants sur leur ordinateur ou en cliquant sur un lien frauduleux) ainsi que sur la trop grande faiblesse des mots de passe utilisés et sur leur trop faible fréquence de mise à jour. Tel est le constat issu de l'analyse des incidents de sécurité de ces dernières années.

C'est pourquoi il est demandé de mettre en œuvre les mesures suivantes dans les délais mentionnés.

1. Règles en matière de sécurité des mots de passe

Tous les mots de passe des personnels, prestataires ou autres comptes génériques utilisés pour accéder aux équipements et services gérés par le ministère, au niveau national comme académique, doivent désormais :

- expirer au bout de 3 ans maximum ;
- être composés d'au moins 12 caractères et inclure au moins une lettre minuscule, une lettre majuscule, un chiffre et un caractère spécial ;
- ne pas être identique aux 3 précédents mots de passe de l'utilisateur (dans les cas où ce critère ne peut pas être techniquement vérifié, il devra faire l'objet de consignes aux utilisateurs).

Au-delà des propriétés des mots de passe, il est recommandé pour les systèmes d'informations sensibles de mettre en œuvre un deuxième facteur d'authentification (code généré par clé OTP[1] ou envoyé par courriel ou SMS[2]...). Pour ce qui concerne les applications nationales, elles sont soumises à la diffusion

[1] Clé OTP (*One-Time Password*) : mot de passe à usage unique généré par une clé physique cryptographique.
[2] *On-Demand Authentification* (ODA) : mot de passe à usage unique envoyé par courriel ou SMS.

de consignes par la DNE quant à leur exposition sur Internet et leurs conditions d'accès : ces consignes sont d'application stricte et ne doivent pas faire l'objet d'adaptions prises localement.

Des règles renforcées doivent par ailleurs être appliquées concernant les comptes ayant des droits « administrateurs » fonctionnels ou techniques sur des systèmes d'information, comme synthétisé dans le tableau suivant :

	Compte utilisateur	Compte administrateur de SI
Durée de validité	3 ans	1 an
Longueur minimale	12 caractères	16 caractères
Réutilisation	3 derniers interdits	10 derniers interdits
Composition	Au moins une minuscule, une majuscule, un chiffre et un caractère spécial	
Multifacteur	Recommandé pour l'accès à des fonctions sensibles	Recommandé dans tous les cas

Je vous remercie de faire respecter ces nouvelles règles aussi rapidement que possible, et dans tous les cas **avant le 21 juin 2024**, pour l'ensemble des personnels exerçant dans les services académiques.

Pour ce qui concerne les personnels enseignants ou exerçant en EPLE, ces nouvelles règles sont à mettre en œuvre **pour la prochaine rentrée scolaire, soit d'ici fin août 2024**.

À ces échéances, aucun mot de passe de plus de 3 ans d'ancienneté ne devra donc subsister.

La mise en place de ces nouvelles règles doit également être l'occasion de sensibiliser à nouveau les personnels aux règles de bonne hygiène en matière de sécurité numérique et de rappeler quelques consignes simples en matière de protection des mots de passe comme :

- ne jamais saisir son mot de passe à la suite de la réception d'un lien dans un courriel (mesure anti-hameçonnage ou *phishing*) ;
- ne jamais stocker des mots de passe de manière non sécurisées (fichier texte, post-it), ni dans un navigateur internet (les dérobeurs de mots de passe ou *stealers* utilisent souvent ces fonctions) ;
- se méfier des logiciels dont l'origine n'est pas garantie, lorsqu'il n'est pas diffusé par son éditeur officiel (ils peuvent être le vecteur pour installer des logiciels malveillants comme des *stealers*) ;
- s'assurer de disposer d'un anti-virus à jour et ne jamais le désactiver ;
- mettre régulièrement à jour ses applications et équipements.

2. Règles en cas d'usurpation d'identité avérée en EPLE

2.1 Concernant les personnels

En cas d'usurpation d'un compte numérique de personnel en EPLE (enseignant ou administratif), le mot de passe du compte doit être réinitialisé dès la connaissance de l'incident. Il est par ailleurs impératif de sensibiliser l'utilisateur concerné sur la **nécessaire vérification de l'intégrité de son ordinateur avant la mise à jour de son mot de passe** : réinitialiser son mot de passe alors que l'ordinateur est infecté par un dérobeur de mot de passe ne ferait que repousser le problème de quelques jours. La nouvelle version de la fiche sur les dérobeurs de mot de passe (*stealers*) ci-jointe pourra être diffusée à cette occasion.

En cas d'incidents multiples sur des comptes de personnels d'un même EPLE, l'ensemble des mots de passe des comptes de personnels de l'EPLE doivent être réinitialisés dans un délai de 5 jours ouvrés, en

lien avec le chef d'établissement, en veillant à accompagner l'opération des mêmes consignes de sécurité indispensables.

2.2 Concernant les usagers (élèves et responsables légaux)

En cas d'usurpation de tout compte numérique d'usager en EPLE (élève ou responsable légal), chaque mot de passe de compte usurpé doit être réinitialisé dès la connaissance de l'incident.

Si survient un second incident impliquant une nouvelle usurpation de comptes dans le même EPLE, l'ensemble des mots de passe des comptes d'accès aux services numériques de vie scolaire et aux environnements de travail numérique (ENT) des usagers de l'EPLE doivent être réinitialisés dans un délai de 10 jours ouvrés, en lien avec le chef d'établissement.

En cas d'usurpation massive de comptes numériques d'élèves ou de responsables légaux touchant plusieurs EPLE dans une période temporelle proche d'un même secteur académique, il est nécessaire d'évaluer puis réaliser une campagne globale de réinitialisation de l'ensemble des comptes du secteur académique.

À ce titre, dans le contexte particulier des vagues actuelles de menaces transmises via les ENT éducatifs depuis mars 2024, le plan de remédiation de crise impose de réaliser pendant la période de congés de printemps, une campagne globale de réinitialisation de l'ensemble des comptes des élèves, des responsables légaux et des personnels sur l'ensemble des ENT éducatifs. Cette action est à mener en lien avec les collectivités territoriales et les chefs d'établissements.

Si la gestion des comptes d'accès n'est pas réalisée par l'EPLE ou les services de l'éducation nationale (cas des ENT ou SI de vie scolaire ne s'appuyant pas sur le service ÉduConnect), il convient de prendre l'attache de la collectivité territoriale ou du partenaire afin de faire procéder à la réinitialisation des comptes d'accès de l'établissement concerné.

Dans tous les cas, ces opérations de remédiation doivent absolument être accompagnées des consignes de sécurité déjà indiquées plus haut, pour éviter que le phénomène ne se reproduise.

Je vous remercie de veiller à l'application de ces consignes dans votre périmètre de responsabilité. Toute difficulté de mise en œuvre est à signaler aux adresses indiquées en tête de cette note.

Le Secrétaire général,
haut fonctionnaire de défense et de sécurité,

Thierry LE GOFF