# Zéro faute
# Cybersécurité, la matière à maîtriser

RÉGION ACADÉMIQUE
AUVERGNE-
RHÔNE-ALPES

*Liberté*
*Égalité*
*Fraternité*

Délégation régionale académique
au numérique éducatif
Site Lyon

# 33 845 noms, prénoms, mails en un mail...


Un parent d'élève du Loiret a reçu un mail via l'ENT avec près de 34 000 adresses mail de collégiens ● © France TV

" J'ai reçu ce mail le 22 mai en fin de matinée d'un expéditeur qui est johndo@moncollege dans lequel il n'y avait pas de sujet. En l'ouvrant, je me suis rendu compte que c'était une liste de mails de collégiens. Il y en a exactement 33 845 lignes", raconte un parent d'une collégienne du Loiret qui a donné l'alerte.

[…] Il alerte sur le fait que cette liste permet selon lui " de **trouver les profils Facebook ou Instagram des élèves, elles servent aussi d'identifiant pour l'ENT. On peut donc se procurer des données personnelles des élèves.** "

Article de France 3 Centre Val de Loire 03/06/2024

# ON SE TESTE !

## Quelle est l'origine probable de la fuite de données personnelles décrite dans l'exemple ?

A) Un piratage

B) Un problème technique du système de messagerie

C) Une erreur humaine

# ON SE TESTE !

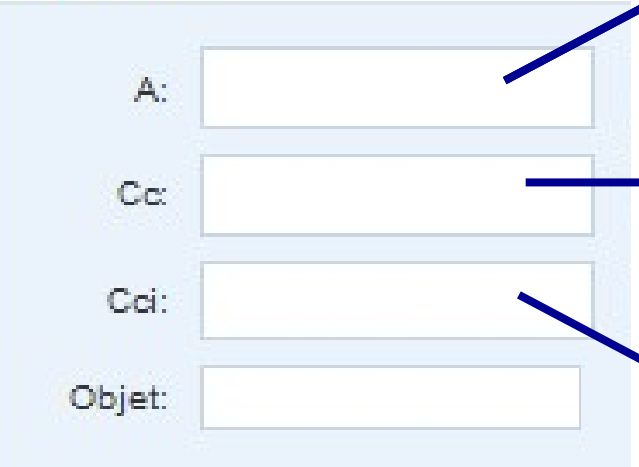
## Quelle est l'origine probable de la fuite de données personnelles décrite dans l'exemple ?

A) Un piratage

B) Un problème technique du système de messagerie

C) Une erreur humaine 

# Choix du champ de destinataire d’un mail




**À**
Destinataire(s) principal(aux)
Ils voient les mails présents dans les champs À et Cc.

**Cc « Copie carbone »**
Destinataires secondaires : mail pour information
Ils voient les mails présents dans les champs À et Cc.

**Cci « Copie carbone invisible »**
Ils voient les mails dans les les champs À et Cc.
Ils ne sont pas vus par les destinataires des champs À et Cc.
Attention ! « Répondre à tous » lève le secret d’envoi !

**Utilisation du Cci**
Pour un envoi massif du mail sans que les destinataires ne voient les adresses mails des autres destinataires ; laisser les autres champs vides.
Exemple : message à destination des parents, des élèves de toute une classe

# Réponse du Rectorat

"En fin d'après-midi ce lundi 3 juin, le Rectorat a répondu par communiqué à notre sollicitation : "Cette erreur de manipulation, lors de l'envoi de messages destinés à appeler les collégiens à la vigilance face aux tentatives de phishing, n'a eu aucune incidence pour les comptes des élèves. Aucun compte n'a été piraté en raison **d'une double sécurité mise en place pour accéder aux Espaces Numériques de Travail**".

Le rectorat explique que l'incident a été **déclaré à la CNIL** et au ministère de l'Éducation Nationale. L'institution tient à rassurer les familles car "aucune conséquence néfaste n'a été enregistrée après cet incident." "

Article de France 3 Centre Val de Loire 03/06/2024

# Un exemple dans l’académie

"
Ce vendredi matin, un piratage informatique d'envergure a eu lieu [dans un établissement de l’académie de Lyon].

**Une ou plusieurs personnes ont réussi à prendre le contrôle du site internet de l'établissement, de l'ENT et Pronote.**

L'une des conséquences majeures fut l'**envoi de faux mails de la part des différents professeurs et membres de la direction.**

Ainsi, les parents ont reçu un courriel de la proviseure adjointe qui leur indiquait que le lycée était fermé "suite à plusieurs explosions dans les différents bâtiments" et que "des mails seront prochainement envoyés aux parents sur la suite de la scolarité de leurs enfants".

Si ce courriel avait un ton cordial et déconnecté de la gravité des faits présumés qu'il relayait, d'autres comme ce professeur de mathématiques ont eu moins de chance avec **le contenu de leurs**

"

**faux mails : une croix gammée, du contenu anti-LGBT […].**


MENU LYONMAG.com

ACCUEIL FIL INFO LYONMAG TV FAITS DIVERS POLITIQUE CONTRIBUTIONS PERSONNALITÉS FORUM ANNO

FAITS DIVERS

Vendredi 15 Mars 2024 à 12h29

Croix gammée et fausses explosions : le site d'un lycée près de Lyon et les adresses mails des profs piratés

Article de LyonMAG 25/03/23

# ON SE TESTE !

**Quelles informations ont été compromises  et ont permis l'envoi des messages ?**

A) L'identifiant et le mot de passe d'un administrateur

B) L'identifiant et le mot de passe d'un élève

C) L'identifiant et le mot de passe d'un professeur

D) Aucune de ces raisons : les pirates ont exploité une faille pronote

# ON SE TESTE !

## Quelles informations ont été compromises  et ont permis l'envoi des messages ?

A) L'identifiant et le mot de passe d'un administrateur 

B) L'identifiant et le mot de passe d'un élève

C) L'identifiant et le mot de passe d'un professeur 

D) Aucune de ces raisons : les pirates ont exploité une faille pronote

# ON SE TESTE !

## Quelles conséquences possibles d'une seule intrusion dans un système informatique ?

A) La perturbation des services, voire l'arrêt de l'activité du service

B) L'inaccessibilité, la destruction, le vol, ou la diffusion des données des enseignants, des parents, des élèves

C) Des risques sociaux et psycho-sociaux pour les personnes exposées

D) La prolongation des vacances scolaires

E) Des risques juridiques : la responsabilité (civile, pénale et administrative) du rectorat peut en effet être engagée

# ON SE TESTE !

## Quelles conséquences possibles d'une seule intrusion dans un système informatique ?

A) La perturbation des services, voire l'arrêt de l'activité du service

B) L'inaccessibilité, la destruction, le vol, ou la diffusion des données des enseignants, des parents, des élèves

C) Des risques sociaux et psycho-sociaux pour les personnes exposées

D) La prolongation des vacances scolaires

E) Des risques juridiques : la responsabilité (civile, pénale et administrative) du rectorat peut en effet être engagée

# Le phishing en vidéo

# ON SE TESTE !

La violation de données personnelles est un incident de sécurité portant sur les données dont un établissement à la charge. Cela peut être une divulgation, une altération, une perte des données personnelles. Elle peut être accidentelle, intentionnelle, malveillante ou non, interne ou externe à l'établissement. Elle a nécessairement des conséquences sur les personnes concernées par la violation, portant atteinte à la confidentialité, l'intégrité ou la disponibilité de leurs données personnelles.

**De combien de temps dispose-t-on pour réagir en cas de violation de données personnelles ?**

A) Immédiatement

B) 3 jours

C) 1 semaine

D) 1 mois

# ON SE TESTE !

La violation de données personnelles est un incident de sécurité portant sur les données dont un établissement à la charge. Cela peut être une divulgation, une altération, une perte des données personnelles. Elle peut être accidentelle, intentionnelle, malveillante ou non, interne ou externe à l'établissement. Elle a nécessairement des conséquences sur les personnes concernées par la violation, portant atteinte à la confidentialité, l'intégrité ou la disponibilité de leurs données personnelles.

**De combien de temps dispose-t-on pour réagir en cas de violation de données personnelles ?**

A) Immédiatement 

B) 3 jours 

C) 1 semaine

D) 1 mois

**Modifier immédiatement son mot de passe et le modifier sur tous les comptes où il a été utilisé !**

# VIOLATION DE DONNÉES PERSONNELLES

Une violation de données personnelles est un incident de sécurité portant sur les données dont un établissement à la charge. Cela peut être une divulgation, une altération, une perte des données personnelles.

Elle peut être accidentelle, intentionnelle, malveillante ou non, interne ou externe à l'établissement.

Elle a nécessairement des conséquences sur les personnes concernées par la violation, portant atteinte à la confidentialité, l'intégrité ou la disponibilité de leurs données personnelles.

RSSI : Responsable de la Sécurité des Systèmes d'Information - dsi@ac-lyon.fr
DPD : Délégué à la Protection des Données - dpd@ac-lyon.fr

## MES RÉFLEXES

En cas de risque élevé, le DPD doit notifier la CNIL dans un délai de 72 heures.


1. Identifier la violation
2. Dater la violation
3. Alerter le DPD et le RSSI
   securite-donnees@ac-lyon.fr
4. Mettre en place des contre-mesures
5. Évaluer la situation avec le DPD et le RSSI
6. Documenter

ACADÉMIE DE LYON
*Liberté*
*Égalité*
*Fraternité*

# ON SE TESTE !

**Quelles sont les 3 pratiques qui sont importantes pour assurer la cybersécurité ?**

A) Utiliser des mots de passe différents et complexes pour chaque site et application

B) Passer la souris sur les liens douteux pour vérifier l'adresse avant de cliquer

C) Activer la double authentification pour sécuriser vos accès, si disponible

D) Envoyer des données personnelles par SMS non chiffré

# ON SE TESTE !

**Quelles sont les 3 pratiques qui sont importantes pour assurer la cybersécurité ?**

A) Utiliser des mots de passe différents et complexes pour chaque site et application

B) Passer la souris sur les liens douteux pour vérifier l'adresse avant de cliquer

C) Activer la double authentification pour sécuriser vos accès, si disponible

D) Envoyer des données personnelles par SMS non chiffré

# Bonnes pratiques

1. Ne **divulguez jamais d'informations sensibles** par courriel ou messagerie non chiffrée.
2. Passez la souris sur les liens douteux pour **vérifier l'adresse avant de cliquer.**
3. En cas de doute, **ne pas cliquer sur les pièces jointes**
4. Vérifiez **l'adresse URL des sites**.
5. En cas de doute, **contactez directement** l'organisme concerné.
6. Utilisez **des mots de passe différents et complexes** pour chaque site et application.
7. Activez la **double authentification** pour sécuriser vos accès, si disponible.

| **Un site pour vérifier les adresses :** | **Signaler :** | **Se faire aider :** |
| --- | --- | --- |
| Phishing initiative | Signal Spam | Cybermalveillance.gouv.fr |

# Sur votre appareil personnel

- **Ne téléchargez pas de programmes ou modules (plug-ins) depuis des sites non-officiel** : ils peuvent contenir des logiciels espions invisibles qui vous volent vos mots de passe (stealer)
- **Appliquez les mises à jour de sécurité** de l'antivirus et du système
- **Supprimez les données personnelles dès que possible** : cela réduit le risque de compromission en cas d'accès non autorisé.
- **Éviter les clés usb** qui se perdent facilement et favoriser le stockage sur l'ENT ou Apps Education.

# Mot de passe robuste

- **Longueur :** 12 à 16 caractères
- **Complexité :** Il doit inclure une combinaison des différents types de caractères (aA&1)
- **Imprévisibilité :** Éviter les mots de passe évidents ou des informations personnelles facilement devinables
- **Passphrases :** Utiliser des phrases de mots aléatoires (par exemple, "ChienBleu!Soleil@Lune123") qui sont plus faciles à retenir tout en restant sécurisées

Comment un mot de passe de 8 caractères est devenu trop faible

# Mot de passe : bonnes pratiques

- Un service, un site ou une application = un mot de passe unique
- Ne plus jamais réutiliser un mot de passe compromis
- Changer les mots de passe régulièrement
- Favoriser l'authentification multi facteur (« MFA »)
- Utiliser un gestionnaire de mot de passe sécurisé pour stocker vos mots de passe

**Découvrez où vos informations personnelles ont fuité et reprenez le contrôle !**
Monitor.mozilla.org

# ON SE TESTE !

**Quelles sont les meilleures pratiques à suivre lors de l'utilisation d'un appareil partagé pour garantir la sécurité de vos informations personnelles ?**

A) Rester connecté à votre session alors que vous quittez la classe

B) Ne pas enregistrer pas vos mots de passe et identifiants dans un navigateur

C) Donner votre identifiant et mot de passe à un collègue pour le dépanner

D) Noter votre mot de passe dans votre carnet de professeur

# ON SE TESTE !

**Quelles sont les meilleures pratiques à suivre lors de l'utilisation d'un appareil partagé pour garantir la sécurité de vos informations personnelles ?**

A) Rester connecté à votre session alors que vous quittez la classe

B) Ne pas enregistrer pas vos mots de passe et identifiants dans un navigateur

C) Donner votre identifiant et mot de passe à un collègue pour le dépanner

D) Noter votre mot de passe dans votre carnet de professeur

# ON SE TESTE !

**Finalement, qui est concerné par la mise en œuvre des pratiques de cybersécurité ?**

A) Les services informatiques du Rectorat et des collectivités (DSI)

B) Les DSI, les personnels de direction et les référents numériques

C) Les DSI et le personnels de l'établissement (direction, professeurs, ...)

D) Les DSI, le personnels de l'établissement, les parents et les élèves

# ON SE TESTE !

**Finalement, qui est concerné par la mise en œuvre des pratiques de cybersécurité ?**

A) Les services informatiques du Rectorat et des collectivités (DSI)

B) Les DSI, les personnels de direction et les référents numériques

C) Les DSI et le personnels de l'établissement (direction, professeurs, ...)

D) Les DSI, le personnels de l'établissement, les parents et les élèves

# C’EST L’HEURE DE CHANGER VOTRE MOT DE PASSE !

https://assistance.ac-lyon.fr/aida/#/

# POUR ALLER PLUS LOIN, RÉALISEZ VOTRE PARCOURS PIX+ÉDU NUMÉRIQUE ET SÉCURITÉ