GUIDE PRATIQUE

LES VIOLATIONS DE DONNEES DANS L'EDUCATION

Version à destination des délégués à la protection des données

Mai 2025

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Table des matières

Introduction

La règlementation sur la **protection des données** s'inscrit dans un contexte de numérisation de la société et repose sur le principe selon lequel « *l'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* »[1].

À travers la notion de **violation de données personnelles**[2], la réglementation prend en compte la possibilité qu'un incident/évènement survienne et rende les données accessibles/utilisables à des tiers, accidentellement ou intentionnellement.

Qu'est-ce qu'une violation de données personnelles ?

D'un côté, il y a des grands principes juridiques :

- Le **droit au respect de la vie privée**, c'est le droit de ne pas être troublé par autrui, que ce soit chez soi ou dans sa sphère d'intimité.
- Une **violation** est une **atteinte** à un droit, à un principe, à un engagement. Dans sa version la plus grave, il existe une volonté de nuire, de faire du tort, à une personne.
- L'**atteinte à la vie privée** regroupe des actions, des comportements (prohibés par la loi) qui portent atteinte à la vie privée (qui pourraient être préjudiciables).

D'un autre côté, il y a les nom, prénom, adresse, numéro de téléphone, etc. : ces informations sont souvent demandées dans le cadre d'activités professionnelles. Ce sont des **données personnelles**.

À partir de ces données, il est possible d'identifier une personne, d'obtenir des informations sur son comportement, sur ses habitudes, sur sa vie privée, etc.

On parle de **violation de données personnelles** quand un **incident** survient et implique des informations sur des personnes physiques : cet évènement va alors nécessiter de s'interroger sur **une possible atteinte à la vie privée**, si une utilisation malveillante de ses informations venait à être faite.

L'évènement déclencheur peut être un **vol**, une **perte**, une **modification** ou une **diffusion non maîtrisée** de données.

Dans le secteur de l'éducation, les établissements scolaires du premier et second degrés mettent en œuvre de nombreux traitements de données personnelles (inscriptions scolaires, environnement numérique de travail, suivi infirmier des élèves…), lesquelles peuvent faire l'objet de violations de données. L'actualité récente montre que les établissements scolaires ne sont pas épargnés par ces incidents. Pourtant, ces cinq dernières années, la CNIL n'a été notifiée que d'une trentaine de violations de données en moyenne par an dans le premier et le second degrés confondus. Lors de ses interventions sur le terrain, la CNIL constate que ce chiffre ne reflète pas la réalité que les établissements vivent au quotidien.

En collaboration avec les délégués à la protection des données (DPO[3]) académiques et le ministère de l'Éducation nationale, la CNIL a réalisé ce guide. Son **objectif** est d'**aider les délégués à la protection des données dans le cadre de l'accompagnement des professionnels de l'éducation et de proposer une démarche à suivre en cas de violation de données**.

Une version similaire de ce guide est mise à disposition des directeurs d'école du premier degré, des chefs d'établissement du second degré, ainsi qu'auprès de son personnel administratif.

---

[1] Article 1er de la loi Informatique et Libertés

[2] Sur cette notion, voir par ex. la vidéo suivante réalisée en 2020 : https://tube-institutionnel.apps.education.fr/w/f7498952-01a4-43ab-bdbb-75bf63a0bbe3

[3] « DPO » pour *Data Protection Officer*, en anglais, ou « DPD » pour Délégué à la Protection des Données.

En complément de ce guide, la CNIL met à disposition des contenus sur la sécurité des données personnelles. Voir notamment :

- le guide de la sécurité des données personnelles[4]. Celui-ci, régulièrement mis à jour, contient notamment des fiches sur la sécurisation des postes de travail et sur la sécurisation du matériel informatique, qui peuvent être mises en œuvre dans les établissements scolaires ;
- le référentiel relatif à la protection de l'enfance[5] en son point 10 (p. 22 – 24). Ce référentiel liste les bonnes pratiques à adopter afin de sécuriser les données concernant des mineurs.

De manière générale sur la sécurité, la CNIL recommande :

- **le chiffrement[6] des disques durs ou des documents**[7] (le chiffrement apporte la garantie minimale que les tiers qui ne connaissent pas le mot de passe ne peuvent pas lire les données) ;
- d'utiliser un **portail sécurisé d'échange de documents** (certaines académies recommandent des outils[8]) ;
- d'utiliser des **mots de passe « robustes**[9] **»** c'est à dire ayant une longueur importante et combinant des caractères alphabétiques en minuscule et en majuscule, des chiffres et des caractères spéciaux (afin de rendre difficilement devinables les mots de passe, y compris par un ordinateur) ;
- d'activer **l'authentification multifacteur**[10] (par exemple par l'envoi d'un SMS à usage unique sur votre téléphone pour valider une connexion) quand elle est proposée ;
- d'apprendre à **vérifier le contenu des messages reçus** (expéditeur, liens hypertextes, etc.).

Que faire en cas de violation de données ?

- ☐ dans **tous les cas**, vous devez analyser et **documenter** l'incident ;
- ☐ si l'incident constitue un **risque** au regard de la vie privée des personnes concernées, l'incident doit être notifié à la CNIL ;
- ☐ en cas de **risque élevé** pour les personnes, le responsable du traitement doit informer les personnes concernées.

---

[4] « Guide de la sécurité des données personnelles », CNIL : https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles
ou en version (PDF, 1,7 Mo) : https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_2024.pdf

[5] *Référentiel relatif aux traitements de données à caractère personnel mis en œuvre dans le cadre de la protection de l'enfance et des jeunes majeurs de moins de vingt-et-un ans* (PDF, 463 ko) :
https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_relatif_a_la_protection_de_lenfance.pdf

[6] Le chiffrement est une mesure de sécurité qui garantit que seules les personnes qui connaissent le code/mot de passe de chiffrement/déchiffrement peuvent lire des informations.

[7] « Comment chiffrer ses documents et ses répertoires », CNIL : https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

[8] Il est préférable d'utiliser des outils recommandés par le ministère ou par RENATER (acteur de référence pour les services numériques pour l'éducation et la recherche). À titre d'exemple :

- « Tutoriel vidéo FileSender », Services Renater : https://services.renater.fr/groupware/filesender/guide_utilisateur/tutoriel_video
- ou « Filesender », Édu-portail de l'académie de Versailles : https://edu-portail.ac-versailles.fr/2018/10/11/filesender/

[9] « Générer un mot de passe solide », CNIL : https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

[10] En demandant plus qu'un mot de passe, ce mode de connexion permet d'ajouter une 2e vérification avant d'accéder au service.

Vol ou perte de matériel informatique ou de documents

*Les supports numériques (**ordinateurs, tablettes, clés USB, disques durs externes**, etc.) et les **documents papier** peuvent contenir des données personnelles des élèves, des familles ou du personnel de l'établissement.*

Les situations fréquemment remontées

Cambriolage dans les locaux

> *Durant le week-end, les bureaux de l'établissement ont été cambriolés. L'ordinateur, la tablette ainsi que la sauvegarde externe ont été volés. Ils contenaient l'intégralité des dossiers élèves (y compris des données de santé d'élèves) et de leurs parents sur plusieurs années. L'ordinateur n'était pas protégé par un mot de passe.*

Vol hors des locaux

> *L'ordinateur portable professionnel du conseiller principal d'éducation de l'établissement a été laissé sans surveillance dans son véhicule et a été volé. Le disque dur de l'ordinateur n'est pas chiffré.*

Oubli dans un espace public

> *L'ordinateur portable personnel de la psychologue a été oublié au restaurant. Il contient les données de suivi des familles en difficulté, et des données de santé des élèves.*

Comment analyser la situation ? (liste non exhaustive)

Des critères d'alerte (constatés dans les notifications) **peuvent aider à évaluer la gravité de la situation :**

- Un disque dur ou support mobile (ex. clé USB) non chiffré[11]**.**
- Un ordinateur dérobé non protégé par un mot de passe.
- Un mot de passe « devinable » ou écrit sur un *post-it***.**
- Des données relatives à la santé physique ou mentale des élèves (PAI, comptes rendus psychologiques, etc.), des informations sur la situation sociale des familles, des données révélant les convictions religieuses, etc.) le numéro de sécurité sociale encadré par le décret n°2019-341 du 19 avril 2019[12], des mesures administratives retenues à l'encontre des élèves, etc.
- Un contexte où une volonté de nuire aux personnes concernées est susceptible d'être en cause.

[11] Le chiffrement est une mesure de sécurité qui garantit que seules les personnes qui connaissent le code/mot de passe de chiffrement/déchiffrement peuvent lire des informations.

[12] En principe, ce numéro ne peut pas être demandé par les établissements scolaires. Voir « Rentrée scolaire : ce que les établissements scolaires et périscolaires peuvent vous demander », CNIL : https://www.cnil.fr/fr/rentree-scolaire-ce-que-les-etablissements-scolaires-et-periscolaires-peuvent-vous-demander. Cependant, en pratique, il arrive qu'il soit collecté et qu'il fasse l'objet d'une violation de données.

Que faire quand l'incident arrive ? (à partir d'exemples de situations)

Vol ou perte de matériel (professionnel, personnel, tablette, etc.) **ou de documents papier contenant des données personnelles** (d'élèves, de familles, etc.)		**Conserver une trace** dans le registre de violations de données	**Notifier la CNIL**	**Informer les personnes**
Les données sur le disque sont chiffrées[13]	Le mot de passe pour déchiffrer n'est **PAS** divulgué (par exemple, il n'est **PAS** écrit sur un post-it avec le matériel dérobé)	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident		
Les données sur le disque sont chiffrées[13]	Le mot de passe pour déchiffrer est sur un post-it avec le matériel dérobé	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓ Si données d'élèves mineurs, de santé, situation sur la famille…	✓ Si possible Individuellement
Les données sur le disque NE sont PAS protégées par du chiffrement		✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓ Si données d'élèves mineurs, de santé, situation sur la famille, …	✓ Si possible Individuellement
Les documents « papier » volés ou perdus contiennent des données « sensibles[14] »		✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓ Si données d'élèves mineurs, de santé, situation sur la famille, …	✓ Individuellement

Les bonnes pratiques essentielles à adopter pour éviter ces situations

- ☐ **Chiffrer les disques durs des ordinateurs ou du matériel mobile utilisé dans les établissements scolaires**[13] (le chiffrement apporte une garantie minimale que des tiers ne peuvent pas lire les données s'ils ne disposent pas du code/mot de passe de déchiffrement).
- ☐ Réaliser des **sauvegardes périodiquement** (la sauvegarde est une copie des données de votre disque. Elle permet de revenir dans une situation de travail « propre », avec le moins de perte possible et permet de savoir qui informer lorsqu'une communication s'avère nécessaire).
- ☐ Activer la fonctionnalité d'effacement des données à distance, quand elle est proposée sur le matériel mobile.
- ☐ **Éteindre** les appareils lorsqu'ils sont laissés **sans surveillance**.

Retrouvez tous nos conseils sur le site web de la CNIL

- « Perte ou vol de matériel informatique nomade : les bons réflexes à avoir ! » : https://www.cnil.fr/fr/perte-ou-vol-de-materiel-informatique-nomade-les-bons-reflexes-avoir
- « Sécurité : Sécuriser l'informatique mobile » : https://www.cnil.fr/fr/securite-securiser-linformatique-mobile

[13] cf. vidéo « comment chiffrer ses documents », CNIL : https://video.cnil.fr/w/wKuisSzFdDdFbKaVNHXWas
[14] Les données sensibles sont les informations qui peuvent s'avérer discriminatoires telles l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données concernant la santé ou des données concernant l'orientation sexuelle d'une personne physique.

L'erreur d'envoi

Il s'agit de situations où une personne partage des informations, de façon non intentionnelle. L'inattention est la principale cause. La prévention est donc importante dans ces cas.

Les situations fréquemment remontées

Courriel adressé à une mauvaise personne

> *Une enseignante a envoyé un message concernant ses élèves et s'est trompée de destinataires : elle a envoyé le message à tous les parents plutôt qu'aux enseignants. Un parent a signalé l'erreur.*

Exemples de facteurs aggravants possibles : le courriel contient des données personnelles de santé ou sur la situation sociale de la famille

Comment analyser la situation ? (liste non exhaustive)

Des critères d'alerte (constatés dans les notifications) **peuvent aider à évaluer la gravité de la situation :**

- Le message dévoile des données de santé physique ou mentale des élèves (PAI, comptes rendus psychologiques, etc.).
- Le message dévoile des données sur la situation sociale ou financière de la famille, le numéro de sécurité sociale encadré par le décret n°2019-341 du 19 avril 2019[15], **les mesures administratives retenues à l'encontre des élèves** ;
- Les données sont ou seront réutilisées par un des destinataires pour une autre finalité ;
- Un contexte où une volonté de nuire aux personnes concernées est susceptible d'être en cause.

Que faire quand l'incident arrive ? (à partir d'exemples de situations)

- ☐ En collaboration avec l'établissement scolaire, contacter les destinataires pour leur demander de supprimer le message et de ne pas utiliser les informations qu'il contenait (si possible et selon la situation, leur demander une attestation écrite).
- ☐ Demander à l'auteur de l'erreur de « faire un rappel des messages » ou d'«annuler l'envoi des messages », si l'outil de messagerie le permet.

L'erreur d'envoi		**Conserver une trace** dans le registre de violations de données	**Notifier la CNIL**	**Informer les personnes**
Seules des adresses courriel sont transmises	Le contenu du message ne révèle pas d'information sur les personnes	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident		

[15] En principe, ce numéro ne peut pas être demandé par les établissements scolaires. Voir « Rentrée scolaire : ce que les établissements scolaires et périscolaires peuvent vous demander », CNIL : https://www.cnil.fr/fr/rentree-scolaire-ce-que-les-etablissements-scolaires-et-periscolaires-peuvent-vous-demander. Cependant, en pratique, il arrive qu'il soit collecté et qu'il fasse l'objet d'une violation de données.

L'erreur d'envoi		**Conserver une trace** dans le registre de violations de données	**Notifier la CNIL**	**Informer les personnes**
Les destinataires ne se connaissent pas	Le message contient des données personnelles (mais hors critères aggravants et Le destinataire a accepté de supprimer les données ou de restituer le document	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident		
Le message révèle des données de **santé**, la situation **sociale** ou **financière** de la famille		✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement
Un **contexte** permettant de supposer une volonté de nuire aux personnes (diffusion sur les réseaux sociaux, réutilisation des données, etc.)		✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement

Les bonnes pratiques essentielles à adopter pour éviter ces situations

- ☐ Chiffrer[16] **les** pièces jointes avec un mot de passe et transmettre le mot de passe par un autre canal
- ☐ Utiliser un portail sécurisé d'échange de documents[17] **ou un outil de communication (de type ENT) pour les échanges entre les familles et l'établissement**
- ☐ Masquer le champ « cc » dans l'outil de messagerie et privilégier la fonction « cci » dans l'outil de messagerie

Retrouvez tous nos conseils sur le site web de la CNIL

- « Le guide de la sécurité des données personnelles » : https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles

[16] Le chiffrement est une mesure de sécurité qui garantit que seules les personnes qui connaissent le code de chiffrement/déchiffrement peuvent lire des informations, ainsi en cas d'erreur d'envoi, le fichier est illisible/indéchiffrable et les données restent protégées.
[17] RENATER (acteur de référence pour les services numériques dans l'éducation et la recherche) recommande un outil accessible sur la page https://services.renater.fr/groupware/filesender/guide_utilisateur/tutoriel_video. Un autre outil est recommandé par l'académie de Versailles https://edu-portail.ac-versailles.fr/2018/10/11/filesender/

L'erreur d'un utilisateur

Il s'agit de situations où une personne effectue une action qui va dévoiler des données, de façon non intentionnelle. La méconnaissance des procédures ou des principes de protection des données en est la principale cause. La sensibilisation est importante, dans ces cas.

Les situations fréquemment remontées

Utilisation d'un outil « public » non sécurisé

> *Un membre de l'équipe administrative a utilisé un outil web de prise de notes, avec reconnaissance vocale, de sorte que les données (d'élèves, de famille, du personnel, etc.) deviennent accessibles sur le web.*

Données rendues publiques

> *Un document destiné à fournir les informations nécessaires à l'enseignant remplaçant a été constitué. Ce document, pour des raisons inconnues, a été publié sur un site internet avec les données élèves et a été indexé par les moteurs de recherche.*

> *Un tiers signale qu'un fichier texte d'une base élève a été publié sur un site web. Des robots d'indexation ont récupéré des informations, de sorte que les données apparaissent lors d'une recherche, via un moteur de recherche.*

Comment analyser la situation ? (liste non exhaustive)

Des critères d'alerte (constatés dans les notifications) **peuvent aider à évaluer la gravité de la situation :**

- Les données de personnes physiques sont facilement accessibles par une recherche avec un moteur de recherche.
- Les données dévoilent des informations sur la situation sociale ou financière de la famille.
- Un contexte où une volonté de nuire aux personnes concernées est susceptible d'être en cause.

Que faire quand l'incident arrive ? (à partir d'exemples de situations)

- ☐ Demander à l'auteur de l'erreur ou demander à l'établissement scolaire d'effectuer une demande de **déréférencement**[18] des données rendues publiques, auprès des moteurs de recherche

[18] Le droit au déréférencement vous permet de demander à un moteur de recherche de supprimer certains résultats de recherche associés à vos noms et prénoms. « Le droit au déréférencement », CNIL : https://www.cnil.fr/fr/comprendre-mes-droits/droit-au-dereferencement

L'erreur d'un utilisateur	**Conserver une trace** dans le registre de violations de données	**Notifier la CNIL**	**Informer les personnes**
Les données ont déjà été rendues publiques **par les personnes**	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident		
Les données révélées sont des données de **mineurs**, de **santé**, relatives à la situation **sociale** ou **financière** de la famille	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement
Un **contexte** permet de supposer une volonté de nuire aux personnes (diffusion sur les réseaux sociaux, réutilisation des données, etc.)	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement

Les bonnes pratiques essentielles à adopter pour éviter ces situations

- ☐ Utiliser les outils référencés par l'éducation nationale **ou les académies**
- ☐ **Éviter les sites non surs ou illicites**

Retrouvez tous nos conseils sur le site web de la CNIL

- « Ma sécurité numérique », CNIL : https://www.cnil.fr/fr/mon-quotidien/ma-securite-numerique
- Poster *Cyber réflexes : se protéger sur Internet* (PDF, 1,4 Mo) : https://www.cnil.fr/sites/cnil/files/2023-10/poster_cyber-reflexes2023.pdf

Le vol d'identifiant et de mot de passe

Il s'agit du comportement d'une personne qui, à des fins malveillantes, va subtiliser les codes d'accès d'un utilisateur.

Les situations fréquemment remontées

Ingénierie sociale / incitation à divulguer des informations

> *Un élève incite une autre élève à lui communiquer ses informations personnelles, notamment son identifiant et son mot de passe. Ces informations sont utilisées pour envoyer des messages injurieux aux professeurs sous le nom de l'élève victime du vol.*

Session laissée ouverte

> *Un enseignant a laissé sa session ouverte : les élèves d'un établissement accèdent à la messagerie, envoient des courriels malveillants, modifient des informations scolaires et accèdent à des sujets d'examen.*

Erreur d'inattention

> *Un enseignant avait laissé à l'écran de son ordinateur la page de connexion à l'ENT faisant apparaitre son identifiant et son mot de passe / à découvert (sur un post-it ou un carnet laissé sans surveillance) ses identifiants et mots de passe pour accéder à son ENT, une élève a pris en photo ces éléments et les a partagés avec des camarades qui ont pu modifier leurs appréciations.*

Utilisation du même mot de passe pour plusieurs comptes

> *Un membre du personnel utilise le même mot de passe pour tous ses services, y compris pour se connecter à l'ENT. Ce mot de passe a été volé lors d'une fuite de données et a été mis en vente. Un tiers malveillant s'est connecté et a utilisé le compte de messagerie pour envoyer des courriels de phishing avec une pièce jointe à toutes les familles. Cette pièce jointe permettait le vol d'identifiant et de mot de passe qui à leur tour ont été mis en vente.*

Couple « identifiant + mot de passe » diffusé

> *À partir du compte usurpé d'une enseignante d'un collège, des courriels injurieux ont été adressés aux parents et aux élèves. Par ailleurs, des notes ont été modifiées sur Pronote et les codes ont été partagés sur un Discord.*

Comment analyser la situation ? (liste non exhaustive)

Des critères d'alerte (constatés dans les notifications) **peuvent aider à évaluer la gravité de la situation :**

- L'utilisateur dont les identifiants ont été volés dispose de droits « étendus » de type « administrateur d'établissement ».
- Un contexte où une volonté de nuire aux personnes concernées est susceptible d'être en cause (envoi de propos injurieux, envoi de messages malveillants, modification des résultats scolaires, etc.).

Que faire quand l'incident arrive ? (à partir d'exemples de situations)

- ☐ **Indiquer à la victime du vol de changer un mot de passe, dès qu'il a perdu son caractère secret/confidentiel**, que ce soit de façon accidentelle ou à la suite d'un acte de malveillance, et de ne plus jamais l'utiliser sur d'autres comptes également, si ce mot de passe est réutilisé pour différents services

Le vol d'identifiant et de mot de passe	**Conserver une trace** dans le registre de violations de données	Notifier la CNIL	Informer les personnes
un mot de passe ou un couple « identifiant + mot de passe » n'est plus « secret »	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ et préciser que le mot de passe ne doit plus être utilisé sur aucune application

Les bonnes pratiques essentielles à adopter pour éviter ces situations

- ☐ Utiliser des **mots de passe « robustes**[19] **»**, c'est à dire ayant une longueur importante et combinant des caractères alphabétiques en minuscule et en majuscule, des chiffres et des caractères spéciaux (afin de rendre difficilement devinables les mots de passe, y compris par un ordinateur).
- ☐ Utiliser un **mot de passe différent pour chaque compte** (si un mot de passe perd sa confidentialité sur un compte alors il ne pourra pas servir sur un autre compte).
- ☐ Conserver ses mots de passe dans un **gestionnaire de mots de passe sécurisé**[20], accessible uniquement après l'utilisation d'un mot de passe maitre (ainsi il n'y a pas besoin de mémoriser tous les mots de passe différents).
- ☐ Activer **l'authentification multifacteur**[21] (par exemple, par l'envoi d'un SMS à usage unique sur votre téléphone pour valider une connexion), quand elle est proposée.
- ☐ Pour les « administrateurs d'ENT », supprimer rapidement les accès des utilisateurs qui ont quitté l'établissement.

Retrouvez tous nos conseils sur le site web de la CNIL

- « Ma sécurité numérique » : https://www.cnil.fr/fr/mon-quotidien/ma-securite-numerique
- « Violation du trimestre : attaque par *credential stuffing* sur un site web » : https://www.cnil.fr/fr/violation-du-trimestre-attaque-par-credential-stuffing-sur-un-site-web

[19] cf. « Générer un mot de passe solide », CNIL : https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

[20] cf. par exemple, l'académie de Paris recommande KeePass XC: https://pia.ac-paris.fr/portail/jcms/p1_3861267/documentation-keepass-xc-methodes-installation (l'accès à la page nécessite une connexion)

[21] En demandant plus qu'un mot de passe, ce mode de connexion permet d'ajouter une 2e vérification avant d'accéder au service.

Les attaques

Il s'agit du comportement d'une personne qui, à des fins malveillantes, va entrer dans une application pour dérober, modifier ou supprimer les données. Être préparé à la possibilité d'une attaque peut s'avérer un élément clé pour réagir efficacement.

Les situations fréquemment remontées

Rançongiciel[22]

> *Les systèmes informatiques d'un établissement ont été la cible d'une attaque par rançongiciel : les données stockées dans ces systèmes ont disparu et seul reste un message demandant le paiement d'une rançon en cryptomonnaie, pour obtenir la clé de déchiffrement et ne pas revendre les données.*

> *Tous les serveurs ainsi que les sauvegardes ont été chiffrés. Les données personnelles impactées sont des données du personnel et les coordonnées des familles d'élèves.*

> *L'analyse technique a révélé que des tentatives d'intrusion de plusieurs comptes utilisateurs avaient été réalisées.*

Vol de données

> *L'ANSSI[23] nous a signalé qu'une base « élèves » est mise en vente sur un site web.*

Site « miroir »

> *Un site miroir d'un ENT à l'identique de l'original a été créé : son adresse est légèrement différente.*
>
> *Pensant accéder à leur ENT, des élèves renseignent leurs identifiants et mots de passe dans le portail frauduleux. Le pirate informatique, auteur de ce faux site, revend les informations de connexion obtenues ou s'en sert pour usurper l'identité des élèves piégés.*

Vol de données obtenu par un programme malveillant

> *Un élève est invité à télécharger, à partir d'une vidéo en ligne, un logiciel / une extension gratuite lui permettant d'améliorer gratuitement ses performances dans un jeu vidéo.*
>
> *Avant le téléchargement, le programme lui demande de désactiver son antivirus. L'élève désactive l'antivirus, télécharge et installe l'extension, ce qui permet au virus (de type « stealer ») de voler ses informations contenues dans son navigateur, y compris ses identifiants et mots de passe d'ENT.*

Attaque par messagerie

> *Un établissement a été victime d'hameçonnage[24]: à partir d'une adresse de messagerie de l'établissement, de nouveaux courriels de phishing ont été envoyés, notamment à un autre établissement.*
>
> *Cela a permis à un tiers non autorisé :*

---

[22] Un rançongiciel (*ransomware* en anglais) est logiciel malveillant qui bloque le bon fonctionnement d'un ordinateur/serveur, tant qu'une rançon n'est pas payée (cf. en annexe du document).

[23] ANSSI (Agence nationale de la sécurité des systèmes d'information) a parmi des missions « d'organiser la protection de la Nation face aux cyberattaques ». Source : « Nos missions », ANSSI : https://cyber.gouv.fr/nos-missions

[24] L'hameçonnage (*phishing* en anglais) est une technique frauduleuse utilisant les systèmes de messageries (courriels, SMS, etc.) destinée à tromper les personnes (cf. en annexe du document).

- *d'avoir accès à la boîte mails de réception de l'établissement, qui contenait notamment des copies des passeports et autres preuves d'identité des enseignants,*
- *d'avoir accès aux noms et adresses, aux coordonnées et aux identifiants de personnes travaillant dans l'établissement,*
- *d'effectuer une campagne d'hameçonnage, avec un lien / une pièce jointe malveillant(e). Le message provenant de l'école inspirait confiance : plusieurs parents ont cliqué / ouvert le message, permettant ainsi la propagation de la compagne d'hameçonnage.*

Comment analyser la situation ? (liste non exhaustive)

Des critères d'alerte (constatés dans les notifications) **peuvent aider à évaluer la gravité de la situation.**

- Pour les « administrateurs ENT », analyser si l'authentification multi-facteur (MFA[25]**)** n'était pas activée.
- Un utilisateur a reçu un courriel de hameçonnage avec une pièce jointe malveillante qu'il a ouvert ou un utilisateur a saisi son identifiant et mot de passe sur une fausse page de connexion.
- des règles de redirection[26] des courriels ont été ajoutées par un tiers.
- un contexte où une volonté de nuire aux personnes concernées est susceptible d'être en cause (envoi de propos injurieux, envoi de messages malveillants, modification des résultats scolaires, menaces terroristes, etc.)

[25] En demandant plus qu'un mot de passe, ce mode de connexion permet d'ajouter une 2e vérification avant d'accéder à l'outil.
[26] Les règles de redirection permettent le transfert de mails à l'attaquant, avec suppression de la boite légitime, pour que l'attaquant envoie un autre courriel (souvent une facture), depuis une adresse courriel ressemblante pour recevoir des fonds.

Que faire quand l'incident arrive ? (à partir d'exemples de situations)

L'attaque avec des conséquences sur les données personnelles			**Conserver une trace** dans le registre de violations de données	**Notifier la CNIL**	**Informer les personnes**
Hameçonnage	Le vol de données est avéré		✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement
Hameçonnage	L'usurpation du compte est avérée	Des messages frauduleux ont été envoyés depuis la messagerie	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement
Hameçonnage	L'usurpation du compte a permis de créer des règles de redirection	Des messages frauduleux ont été envoyés depuis la messagerie	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement
Rançongiciel	Selon les analyses techniques, il n'y a pas eu de vol de données	Sauvegardes **saines** disponibles	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	
rançongiciel	Selon les analyses techniques, il y a un doute quant à un vol de données		✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement
Rançongiciel	Le vol de données est avéré	les données sont mises en vente sur le web	✓ Documenter les mesures prises ou annoncées pour prévenir un nouvel incident	✓	✓ Individuellement

Les bonnes pratiques essentielles à adopter pour éviter ces situations

- ☐ Apprendre à reconnaitre un message d'hameçonnage[27] **(expéditeur, liens hypertextes, etc.)**
- ☐ En cas de doute, à réception d'un message (courriel, SMS, etc.), prendre le temps de contacter la personne directement ou par un autre canal
- ☐ Se connecter depuis le site officiel (taper l'URL ou conserver l'adresse dans les favoris) plutôt que depuis un lien reçu par courriel ou résultat d'un moteur de recherche[28]
- ☐ **Ne pas installer de programmes dont l'origine est douteuse**[29]
- ☐ Contacter le service informatique avant toute installation de logiciel qui n'est pas expressément autorisé, sur le matériel professionnel
- ☐ Installer un antivirus et faire régulièrement les mises à jour de vos appareils, logiciels et applications
- ☐ Apprendre à gérer ses mots de passe de façon sécurisée[30]

Retrouvez tous nos conseils sur les sites web de la CNIL et de cybermalveillance.gouv.fr

- « Violation du trimestre : les attaques sur les messageries », CNIL : https://www.cnil.fr/fr/violation-du-trimestre-les-attaques-sur-les-messageries
- « Rançongiciel ou ransomware, que faire ? », Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

[27] Voir « *Spam*, *phishing*, arnaques : signaler pour agir », CNIL : https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir ou « Que faire en cas de phishing ou hameçonnage ? », Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

[28] Attention aux sites « miroir » qui sont des copies de sites légitimes !

[29] Poster *Cyber réflexes. Se protéger sur Internet* (PDF, 1,4 Mo), CNIL : https://www.cnil.fr/sites/cnil/files/2023-10/poster_cyber-reflexes2023.pdf

[30] « Les conseils de la CNIL pour un bon mot de passe », CNIL : https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

Annexe 1 : Les notions clés

Focus sur le rançongiciel

Une fois entrés dans un système informatique, les tiers peuvent :

- copier, détruire ou modifier des données qui s'y trouvaient;
- installer des logiciels malveillants, qui leur permettent d'accéder au système, ultérieurement (durant la nuit ou le week-end, par exemple).

Les conséquences d'une telle attaque ne seront pas immédiatement claires. Toutefois, pour les utilisateurs, la conséquence visible est la perte des données et la demande de paiement d'une rançon dans le seul fichier texte lisible.

Pour déterminer quelles données personnelles ont été touchées, il convient :

- de réaliser un **dépôt de plainte ;**
- de **contacter les équipes informatiques**[31], qui pourront à leur tour contacter le CSIRT[32] régional pour être mis en relation avec des prestataires de réponse à incident de sécurité.

Dans le cas le plus favorable, les investigations techniques concluront qu'il n'y a pas eu de vol de données et des sauvegardes permettront de remettre en fonctionnement le système.

Dans le cas le plus défavorable, les données seront proposées sur un site de revente de données.

Focus sur l'hameçonnage

L'hameçonnage ou phishing est une forme d'escroquerie.

Les messages d'hameçonnage sont fréquemment conçus pour être quasi-similaires aux messages de l'organisme dont ils ont usurpé l'identité. Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en reproduisant sa charte graphique (en utilisant le logo, le nom de cet organisme, etc.).

Il vous envoie un mail vous demandant généralement de « mettre à jour » ou de « confirmer vos informations suite à un incident technique », notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.). Le contenu peut également être inquiétant et inclure une incitation à cliquer sur un lien (qui semble rediriger vers la page officielle d'un site).

Même si seuls les noms et les adresses électroniques sont dérobés, ces données peuvent être utilisées par le tiers pour mener de nouvelles attaques de *spam*, de *phishing* (via courriel, via SMS, etc.), de vols d'identifiants et mots de passe, etc. Un courriel provenant d'une adresse de du monde de l'éducation/enseignement pourrait facilement être assimilé à une personne de confiance : il sera alors important d'alerter rapidement les destinataires, en cas d'usurpation d'un compte, afin de limiter les risques de propagation.

Attention cependant, en cas de courriel envoyé à des mineurs à ne pas produire l'effet inverse de l'effet voulu (c'est-à-dire que le fait de les prévenir les incitent à aller voir le contenu piraté. Dans le cadre des environnement numériques de travail (ENT) il peut être efficace de prévenir le prestataire qui peut effacer ce type de contenu.

Conséquences possibles d'un vol de données avec une mise en vente sur le marché noir

Les données personnelles volées peuvent être ajoutées et croisées avec des données existantes qui sont déjà vendues sur le marché noir, par exemple.

---

[31] Selon l'organisation, ce pourrait être le prestataire informatique, le responsable de la sécurité des systèmes d'informations (RSSI), l'équipe CSIRT (*Computer security incident response team*)

[32] Les CSIRT régionaux (https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux/) sont des centres de réponse aux incidents cyber au profit des entités implantées sur le territoire régional. Ils traitent les demandes d'assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations). L'émergence de ces CSIRT doit permettre de fournir localement un service de réponse à incident de premier niveau gratuit, complémentaire de celui proposé par les prestataires, la plateforme Cybermalveillance.gouv.fr et les services du CERT-FR.

Ces données sont ensuite éventuellement utilisées dans des listes de spam ou dans des attaques, pour tenter d'accéder à des comptes d'utilisateurs auprès d'autres organisations, telles que des banques, des boutiques en ligne ou des détaillants, en utilisant des informations précédemment divulguées.

Annexe 2 : Les ressources des académies sur la sécurité des données

- https://cybersecurite.toutatice.fr : site de cybersécurité de l'académie de Rennes où retrouver les newsletters envoyées entre chaque vacance scolaire aux usagers de l'académie.
- https://dane.ac-reims.fr/index.php/responsabiliser/rgpd : page RGPD du site de la région académique Grand-Est. Une vidéo, réalisée en 2020, https://tube-institutionnel.apps.education.fr/w/f7498952-01a4-43ab-bdbb-75bf63a0bbe3 présente la notion de violation de données.