Perte ou vol de matériel informatique nomade : les bons réflexes à avoir !

15 septembre 2022

Régulièrement, la CNIL communique sur des violations de données typiques inspirées d'incidents réels qui lui sont notifiés. La présente publication a pour objectif d'expliquer comment se protéger lors de l'utilisation de supports amovibles pouvant contenir des données personnelles.

Le recours à du matériel informatique nomade pouvant contenir des données personnelles est aujourd'hui courant. Cela va de l'utilisation de clés USB, de disques durs externes au déploiement massif de flottes d'ordinateurs portables ou encore de smartphones. Cette tendance s'est d'autant plus renforcée avec le développement accéléré du télétravail.

Si cette évolution répond à de réels besoins, elle engendre des risques particuliers dus aux risques de perte ou de vol dans l'espace public, hors de l'espace sécurisé de l'entreprise.

Heureusement, il est relativement simple et peu coûteux de sécuriser les données contenues dans ce matériel en cas de perte ou de vol. Une check-list en fin de page rappelle les bonnes pratiques à appliquer.

PERTE OU VOL DE MATÉRIEL INFORMATIQUE NOMADE : COMMENT RÉAGIR ?

Lucie est responsable SSI d'une entreprise cosmétique.

Un employé prévient Lucie du vol de son ordinateur. Ils s'entretiennent afin d'évaluer les risques liés aux données personnelles.

Lucie contacte Nabil, le délégué à la protections des données de l'entreprise, et se répartissent les tâches.

MOT DE PASSE ROBUSTE

****

PORTS USB ET BIOS ACCESSIBLES !

Elle analyse les risques d'accès : l'ordinateur était éteint et protégé par un mot de passe robuste. Mais les ports USB et l'accès au BIOS ne sont pas bloqués.

Elle réinitialise le mot de passe de l'employé et révoque ses accès VPN, tout en tenant Nabil informé.

Bonjour Nabil

Lucie O. RSSI

J'ai fait tout le nécessaire sur le poste de l'employé

Lucie O. RSSI

Et je n'ai détecté aucune activité sur son ordi portable

Lucie O. RSSI

Très bien, merci Lucie !

Nabil L. DPO

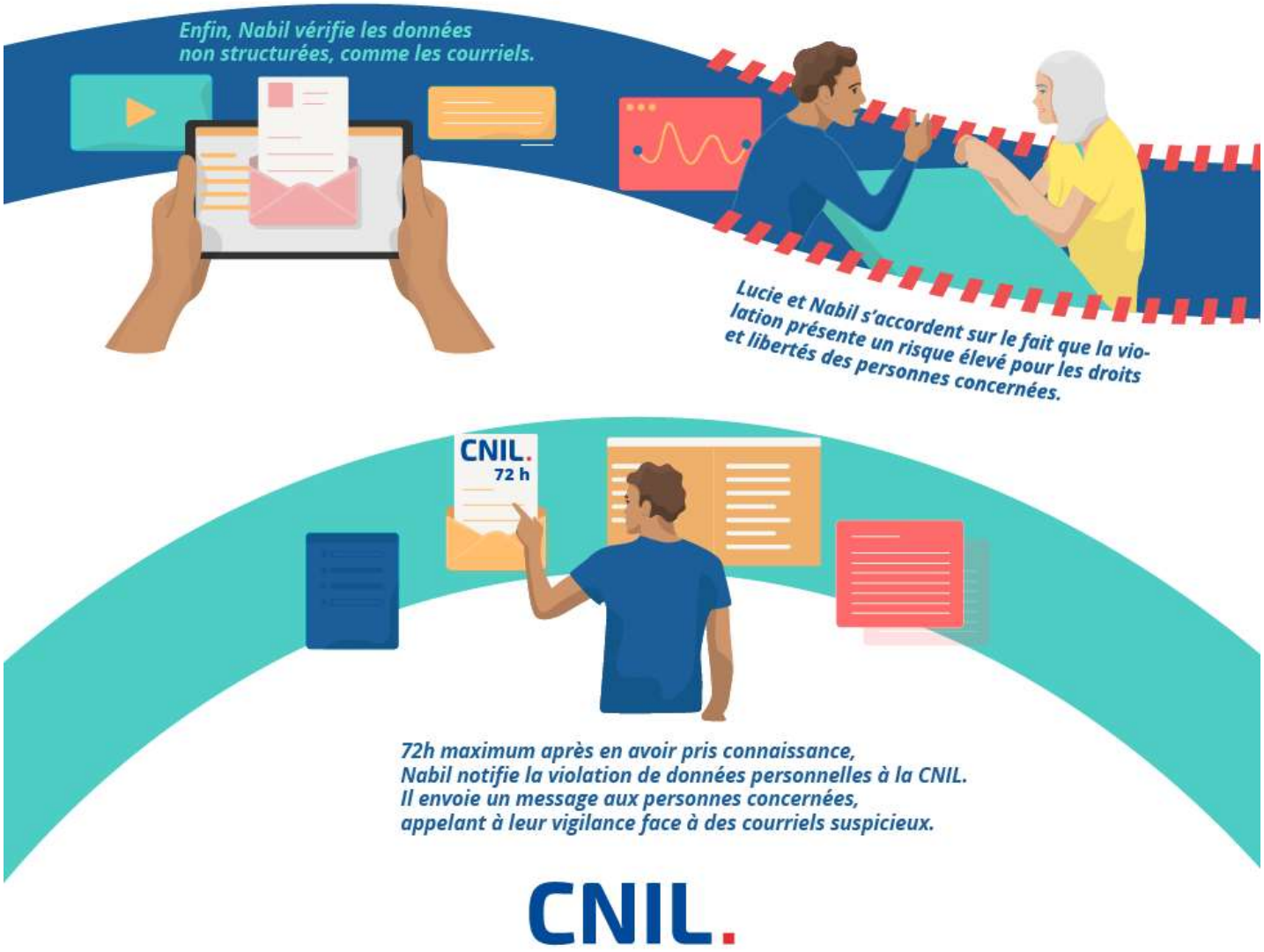
L'employé avait notamment conservé sur son poste des coordonnées bancaires et d'autres informations personnelles de clients.

gestionnaire de mots de passe

identifiant

****

Nabil répertorie les applicatifs auxquels l'employé avait accès, et vérifie s'il utilisait un gestionnaire de mot de passe sécurisé.



Découvrir toute l'histoire de Lucie et Nabil

Une situation classique

Lucie est responsable de la sécurité des systèmes d'information au sein d'une grande entreprise de cosmétiques. Avec le développement du télétravail, de plus en plus de salariés de la société sont équipés d'ordinateurs portables et de smartphone et amenés à se déplacer avec ces derniers.

Lundi matin, en arrivant au bureau, elle reçoit un courriel d'un manager lui indiquant qu'un membre de son équipe a été victime d'un cambriolage à son domicile, pendant le week-end et que, parmi les affaires qui lui ont été dérobées, se trouve l'ordinateur portable mis à sa disposition par l'entreprise.

Lucie connaît bien la procédure à suivre à la suite d'un tel incident, elle l'a écrite elle-même ! Elle prend alors contact avec le manager et arrange un entretien avec l'employé victime afin de vérifier avec lui quelle est sa fonction et quelles sont les applicatifs auxquels il a accès. Malheureusement pour Lucie et l'entreprise, l'employé victime était équipé d'un matériel nomade depuis longtemps, et ne disposait donc pas d'un des équipements récemment mis en place avec une surcouche de sécurité.

En effet, depuis qu'elle a pris ses fonctions l'année précédente, Lucie a mis en place une procédure de gestion des équipements mobiles au sein de son entreprise. Cette tâche lui a paru **nécessaire et simple**, étant issue d'une entreprise où une telle procédure était suivie depuis longtemps. Ainsi, toutes nouvelle personne prenant ses fonctions ou faisant l'objet d'un renouvellement de son matériel dispose dorénavant d'un ordinateur dont le disque dur est entièrement chiffré.

Cependant, dans le cas présent, le renouvellement du matériel ne s'effectuant que tous les 3 ans, ce dernier ne disposait pas de ces protections. Lucie a par ailleurs conscience que plus l'employé a de l'ancienneté dans l'entreprise, plus il a des chances que son ordinateur contienne une masse importante d'informations, notamment des données personnelles - l'employé en question travaillant, de plus, au service client. Comme le prévoit la procédure, elle **contacte sans attendre Nabil,** le délégué à la protection des données (DPO) de l'entreprise, afin de gérer cet incident de sécurité.

Comment Lucie et Nabil doivent-ils réagir pour faire face aux risques ?

Après s'être entretenus avec l'employé, Lucie et Nabil se répartissent les tâches.

Du côté de Lucie, la RSSI : vérifier les informations relatives à la sécurité du matériel

Lucie sait que **l'ordinateur était éteint** et que ce dernier est **protégé par un mot de passe robuste**. Il y a peu de probabilité que le voleur puisse, si tel était son souhait, accéder aux informations contenues sur la machine en la démarrant.

Cependant, elle sait également que **ni les ports USB ni l'accès au BIOS ne sont bloqués** : une personne avec des connaissances techniques pourrait facilement accéder au contenu du disque en démarrant, par exemple, depuis une clé USB ou en démontant le disque dur et en le connectant sur une autre machine.

Enfin, elle sait que le poste de l'employé au service client n'est **pas un poste sensible** et que ce dernier l'a informé que ses voisins avaient également été touchés par des cambriolages : Lucie, après en avoir discuté avec Nabil, part du postulat qu'il s'agit d'un vol **non ciblé** sur l'entreprise et ses données. Ces **informations de contexte sont prises en compte dans leurs analyses de risque**, qui visent tant à déterminer le risque pour l'entreprise que pour les personnes dont les données sont stockées sur le poste.

Lucie **réinitialise le mot de passe du domaine** de l'employé et **révoque ses accès distants (VPN)**.

Du côté de Nabil, le DPO : vérifier les risques pour les données personnelles

Pendant ce temps, Nabil **répertorie les applicatifs** auxquels l'employé avait accès. Il constate que la victime n'avait **pas enregistré les identifiants et mots de passes des applicatifs web au sein de son navigateur**, conformément à la charte informatique. Cependant, **il n'utilisait pas de gestionnaire de mot de passe sécurisé**.

L'employé confirme également qu'**il n'avait pas effectué de copies locales de documents et de données issues des répertoires partagés** sur son poste, préférant travailler dans des dossiers partagés en étant toujours connecté au VPN pour bénéficier de sauvegardes régulières. Cette information rassure Nabil : **il ne semble pas, à ce stade, qu'il y ait une perte d'information (atteinte à la disponibilité)**.

Cependant, afin de réaliser des opérations de suivi et d'appel à facturation, ce dernier avait tout de même extrait des informations au format tableur sur son poste. Ces fichiers contenaient notamment des informations personnelles tel que des données d'état civil mais également bancaires (RIB, IBAN, appel à facturation, etc.) et concernaient les opérations traitées durant les trois derniers mois.

Ce qui inquiète Nabil maintenant, ce sont **les données non structurées, comme les messages**. Au service client, les échanges par courriels sont nombreux et il est difficile de savoir ce qui se trouve dans la boîte de l'employé. Avec l'aide de Nabil et de son manager, l'employé tente maintenant de déterminer quelles informations, notamment personnelles, sont concernées. De ce côté-là, une **perte d'information** pourrait être enregistrée, l'employé ayant pour des archives locales de ses courriels les plus anciens, qui ne se trouvent pas sur le serveur et qui ne sont pas sauvegardées.

La mise en commun des investigations de Lucie et Nabil

De son côté, Lucie confirme a Nabil qu'elle n'a pas détecté d'activité issue de ce poste dans les journaux centraux de connexions depuis le vendredi en fin d'après-midi. Le poste de travail n'a donc pas été utilisé pour accéder au SI de l'entreprise après le vol.

Les investigations continuent, Nabil informe Lucie qu'il va maintenant falloir se pencher sur l'aspect légal : après échanges, ils s'accordent sur le fait que **la violation présente un risque pour les droits et libertés des personnes concernées**, et que ce risque, à partir des informations à leur disposition à ce stade, peut être considéré comme élevé. Effectivement, les données de facturation peuvent permettre à un attaquant de tenter d'effectuer des arnaques de type faux ordre de virement international ou FOVI (communément appelé « fraude au président »). Nabil est particulièrement attentif à cette menace, ayant connaissance de la publication récente de la CNIL sur le sujet.

Ainsi, **dans les 72 heures suivant la prise de connaissance de la violation de données personnelles** (la prise de connaissance étant le lundi lorsque l'employé de retour de week-end s'est aperçu du méfait et a informé son manager), **Nabil effectue une notification initiale de violation de données personnelles à la CNIL**. De plus, avec l'aide du service communication, après en avoir référé à sa hiérarchie qui a donné son feu vert, il réalise un message d'information pour les personnes concernées, appelant à leur vigilance en cas de réception de courriels suspicieux.

Comment limiter le risque en cas de vol ou de perte de matériel ?

Pour éviter de vous retrouver dans la situation de Nabil et Lucie, voici ce qu'il est conseillé de faire :

1. **Gérer son parc et les ressources de ses utilisateurs**

✅ Savoir quel matériel est affecté à quelle personne.

✅ Connaître les matrices d'accès qui sont affectées à chaque profil (quel profil ou quelle fonction de l'entreprise accède à quel logiciel ou à quelle ressource réseau ? Etc.)

✅ Avoir à sa disposition les outils permettant de gérer les accès et avoir la possibilité de les révoquer.

✅ Lorsque cela n'est pas nécessaire, empêcher le démarrage (boot) depuis les ports USB et protéger l'accès au BIOS des postes de travail par un mot de passe.

2. **Mettre en place des procédures d'authentification**

✅Mettre en place un dispositif d'authentification robuste. Si l'authentification se fait par couple identifiant et mot de passe, respecter les recommandations de la CNIL et celles de l'ANSSI sur le sujet.

✅ Ne pas stocker ses identifiants et mots de passe au sein de ses navigateurs (et encore moins sur un post-it collé sur clavier !).

✅ Mettre à disposition des utilisateurs des gestionnaires de mots de passe sécurisés.

3. **Chiffrer les données**

✅ Chiffrer les données sur les postes nomades. Aujourd'hui, l'immense majorité des systèmes d'exploitation propose en standard des mesures de chiffrement faciles à mettre en œuvre.

✅ Chiffrer les données au repos des supports amovibles, comme les clé USB ou disques dur. L'ANSSI propose des solutions afin de faciliter la mise en œuvre de ce type de mesure.

✅ Mettre en place une procédure de gestion des clés cryptographiques : les clés de chiffrement des matériels nomades doivent être sauvegardées par le service informatique en cas d'oubli par les salariés.

4. **Effectuer des sauvegardes régulières**

✅ Prévoir, mettre en place **et tester** une procédure de sauvegarde des postes nomades lorsque ces derniers se connectent au réseau de l'entreprise.

5. **Sensibiliser les utilisateurs**

✅ Sensibiliser régulièrement les salariés sur les risques liés à la perte d'un support contenant des données personnelles et des donnés d'entreprise, par exemple par un envoi de mails réguliers à l'ensemble du personnel.

✅ Former les personnes amenées à manipuler des données stockées sur des supports amovibles et les inciter à signaler la perte ou le vol de leur matériel.

Texte reference

Pour approfondir

> Les violations de données personnelles
> Tous les contenus sur la cybersécurité
> La CNIL publie une recommandation relative aux mesures de journalisation
> Sécuriser l'informatique mobile
> Protéger ses appareils mobiles – cybermalveillance.gouv.fr
> Bonnes pratiques à l'usage des professionnels en déplacement - ANSSI