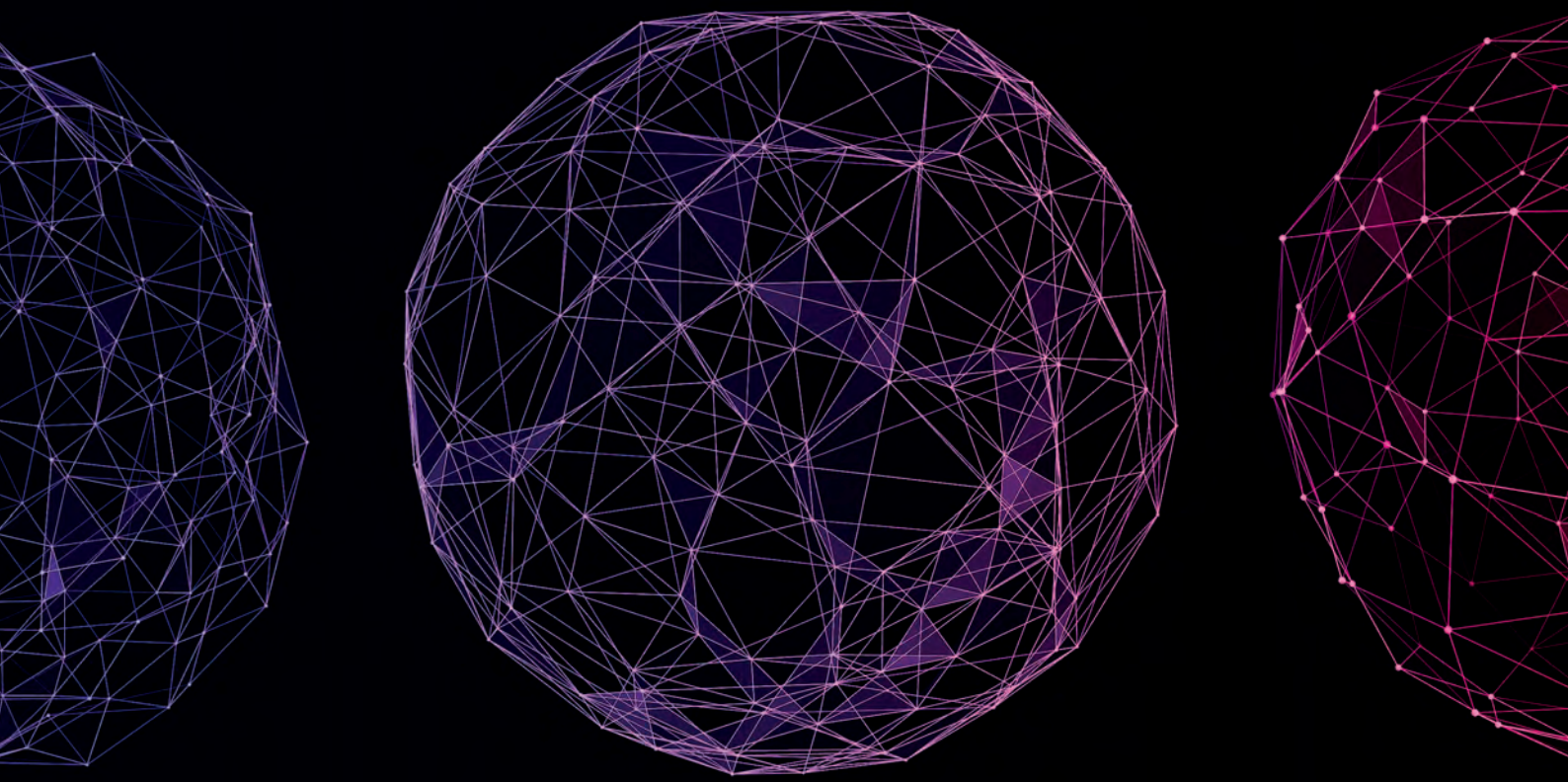
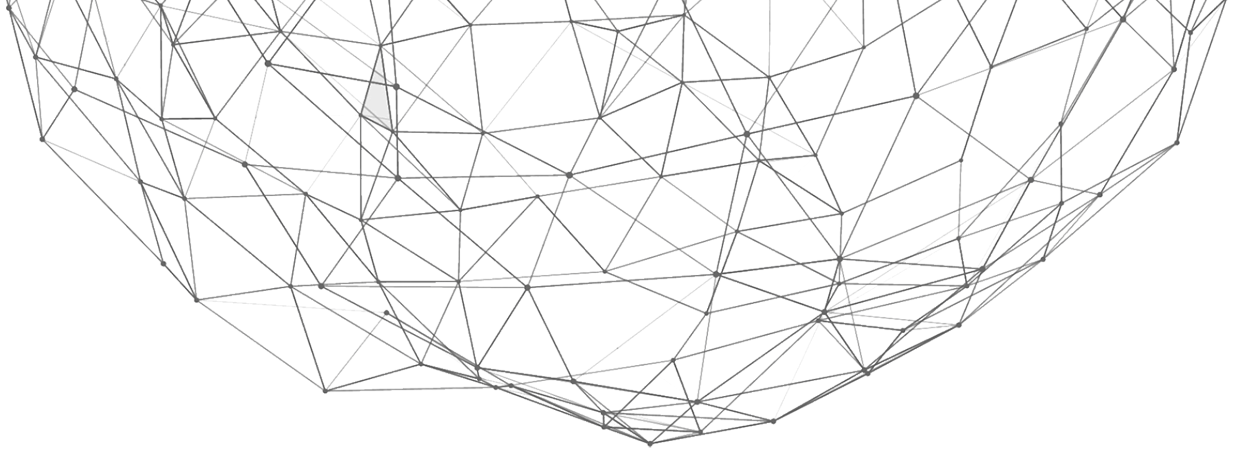
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État

MEMENTO DES BONNES PRATIQUES



PRÉVENTION ET GESTION DES INCIDENTS DE SÉCURITÉ ET DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL



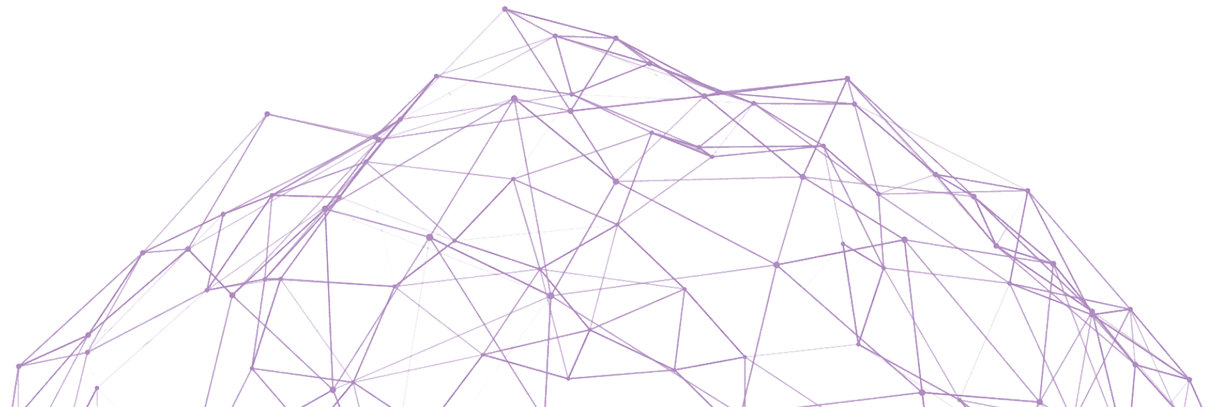
Cette publication élaborée par le Commissariat du gouvernement à la protection des données auprès de l'Etat (« CGPD ») contient les principales bonnes pratiques à respecter par les agents dans le cadre de la prévention et de la gestion des incidents de sécurité et des violations de données à caractère personnel. Elle est le fruit d'une étroite collaboration entre les acteurs clés impliqués dans la sécurité de l'information, la protection des données à caractère personnel ainsi que la gestion des incidents de sécurité.

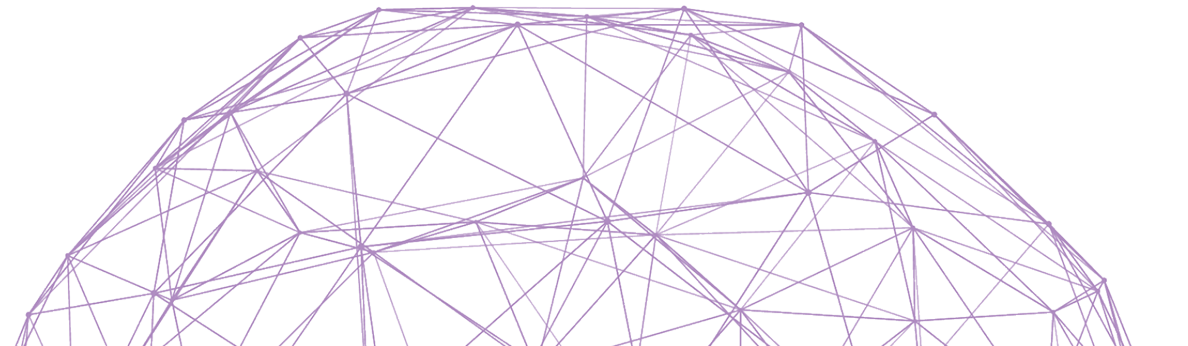
Pour des informations plus détaillées en la matière, veuillez consulter la publication « Prévention et gestion des incidents de sécurité et des violations de données à caractère personnel » du CGPD.

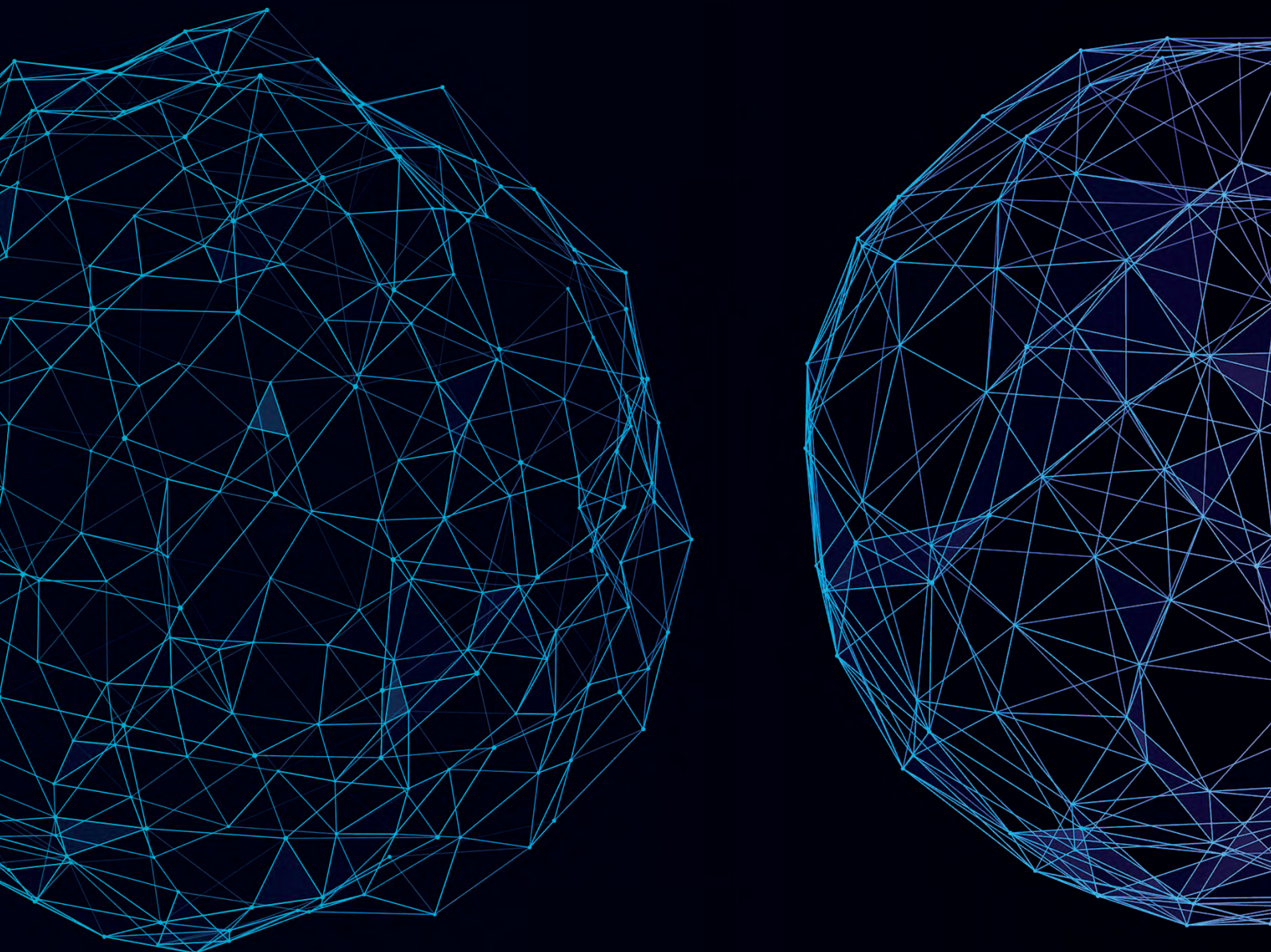
Les acteurs ayant participé à l'élaboration de la présente publication sont :

- le Haut-Commissariat à la protection nationale,
- l'Agence nationale de la sécurité des systèmes d'information,
- le Centre de traitement des urgences informatiques (« GOVCERT »),
- le Centre des technologies de l'information de l'Etat,
- la Luxembourg House of Cybersecurity,
- l'Institut luxembourgeois de régulation,
- la Commission nationale pour la protection des données,
- le Centre commun de la sécurité sociale.

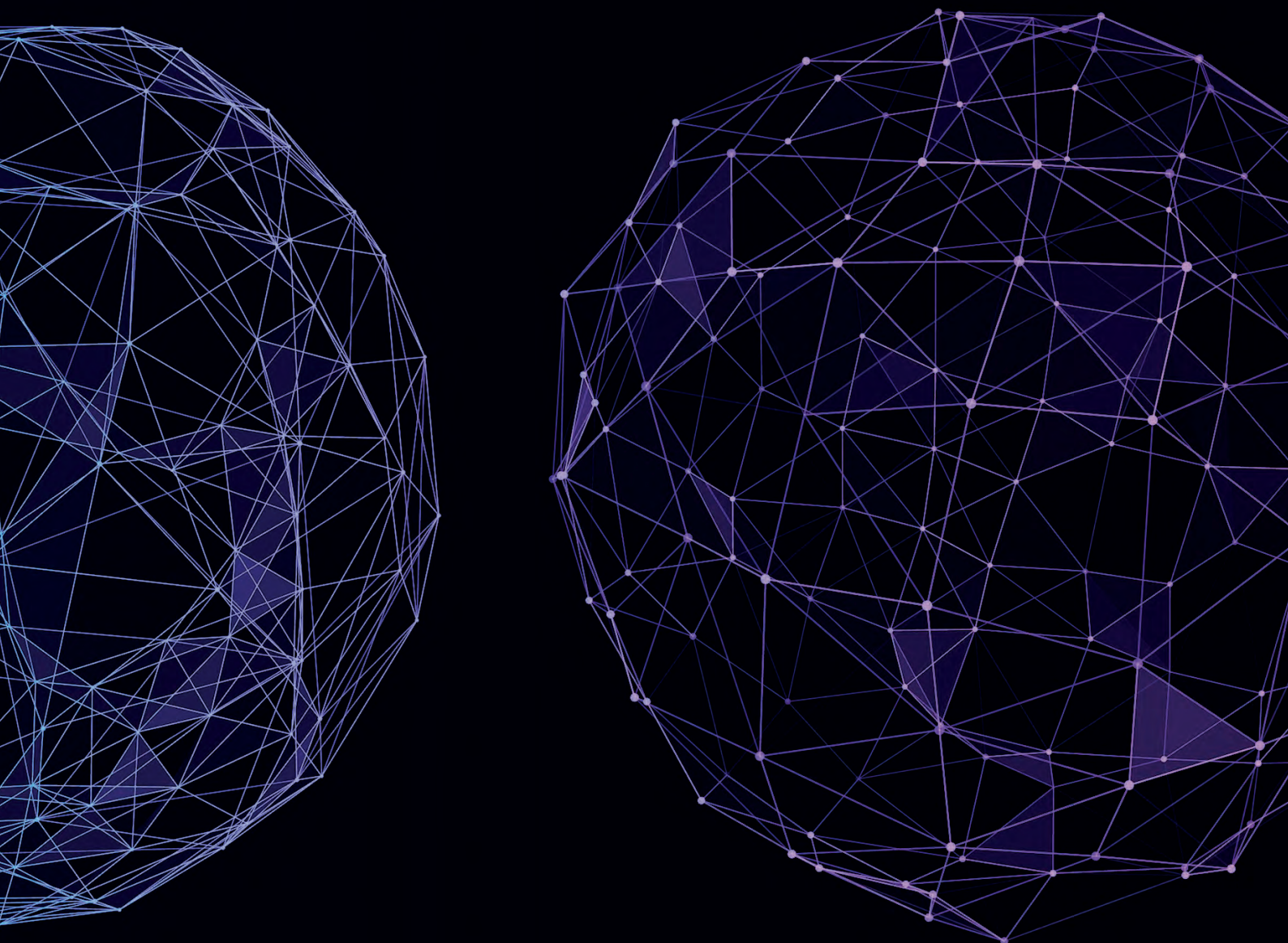
TABLE DES MATIÈRES







INTRODUCTION//



INTRODUCTION //

La sécurité de l'information constitue un volet essentiel de la protection des infrastructures nationales, des données à caractère personnel et, de manière plus générale, des intérêts nationaux luxembourgeois et européens. Elle est indispensable pour consolider la confiance des citoyens et des administrés dans les institutions et services publics, en particulier dans le contexte de la digitalisation de l'administration publique.

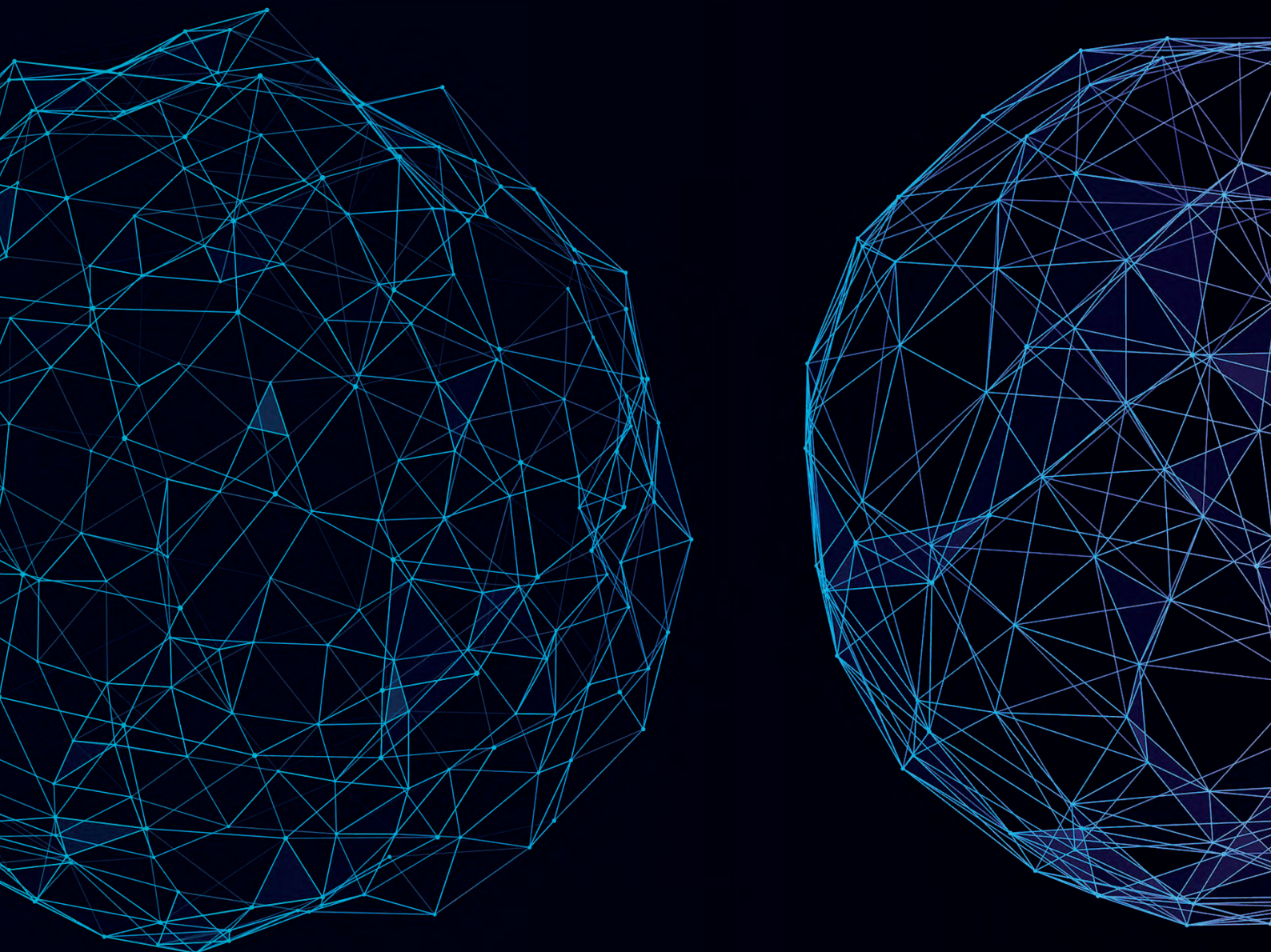
Il est primordial que les agents de la fonction publique soient sensibilisés à la sécurité de l'information et des données à caractère personnel. Ils doivent être conscients des risques qui peuvent résulter de comportements inappropriés dans la gestion des informations et données à caractère personnel.

En effet, ***un agent bien sensibilisé en la matière contribue à la relation de confiance*** *qui doit impérativement subsister entre les citoyens et l'administration.*

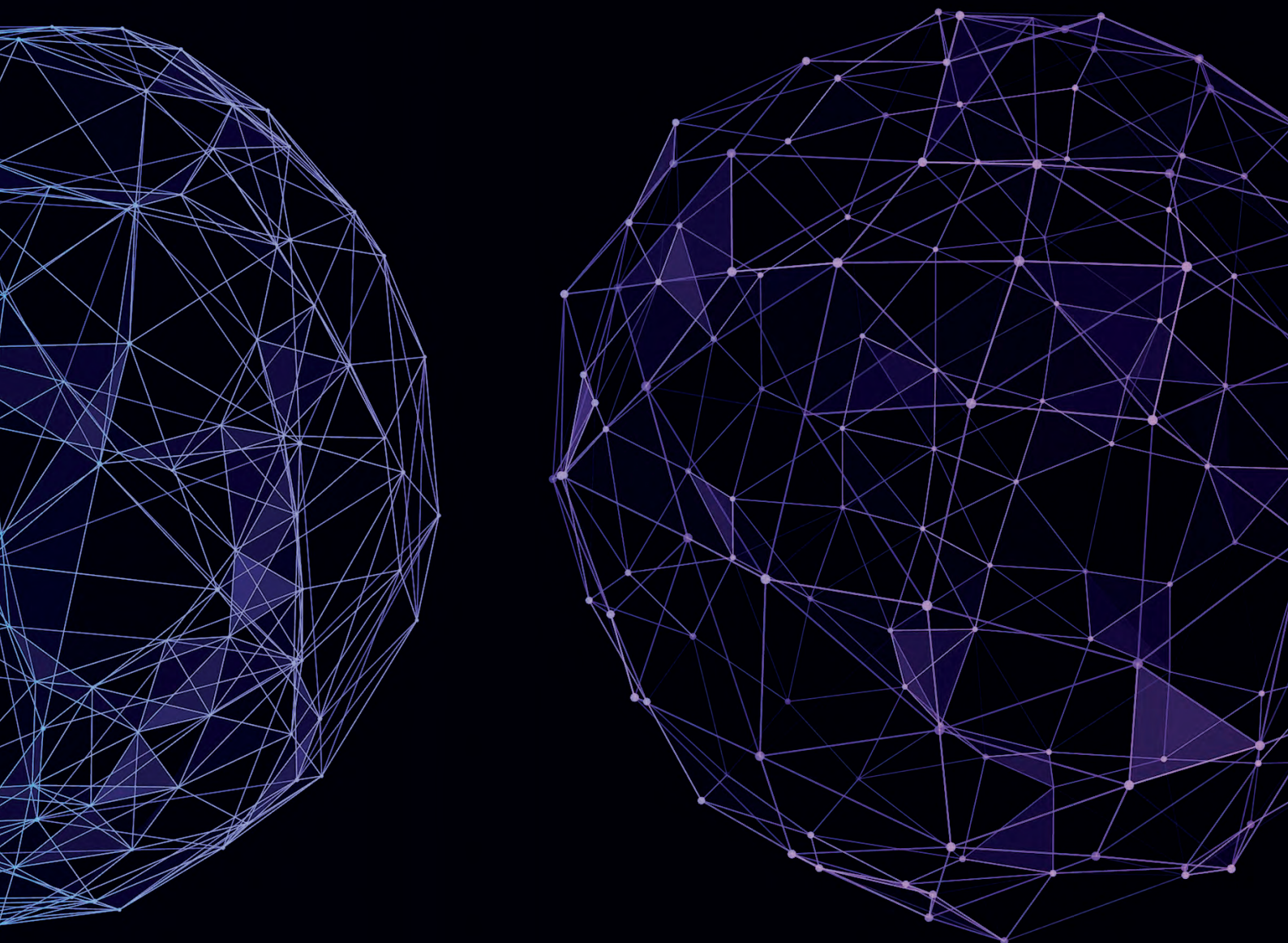
L'agent est tenu de se conformer consciencieusement aux lois et règlements qui encadrent l'exercice de ses fonctions, aux instructions du gouvernement qui ont pour objet l'accomplissement régulier de ses devoirs ainsi qu'aux ordres de service de ses supérieurs (loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat).

L'agent a **une obligation de discrétion et de secret professionnel**. Il ne doit pas révéler les faits dont il a obtenu connaissance en raison de ses fonctions et qui auraient un caractère secret de par leur nature ou de par les prescriptions de ses supérieurs hiérarchiques, à moins d'en être dispensé par le ministre du ressort.

De ce fait, toute transmission ou divulgation de données est proscrite si le destinataire (interne ou externe à l'administration) ne remplit pas, au moment de la réception des données, les conditions dans lesquelles il est habilité à les traiter. En outre, **l'agent doit traiter les données dans les strictes limites des missions d'intérêt public poursuivies par l'administration et pour les seuls objectifs fixés par celle-ci. Tout détournement et toute communication à des tiers contraires aux lois et règlements sont interdits.**

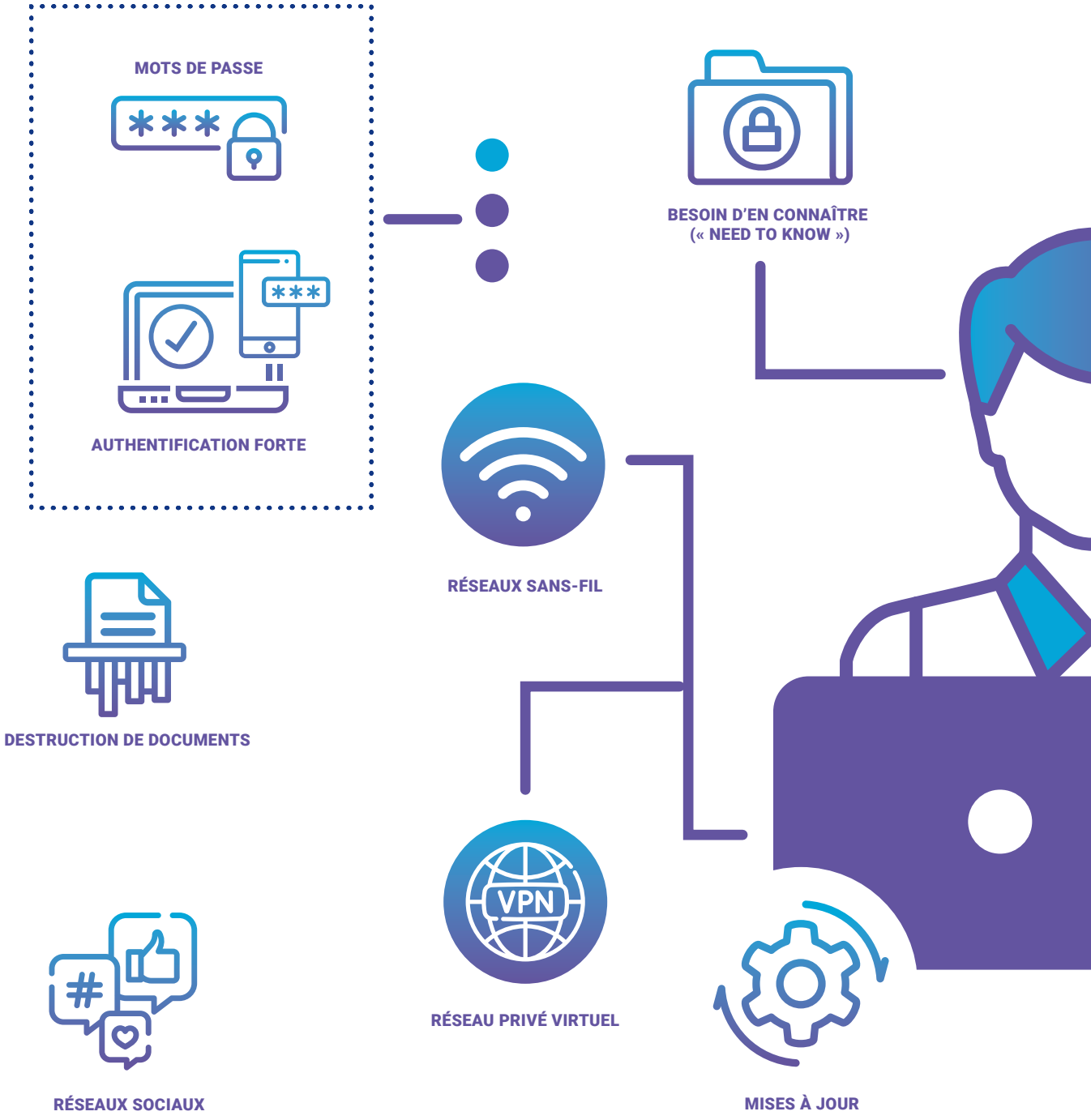


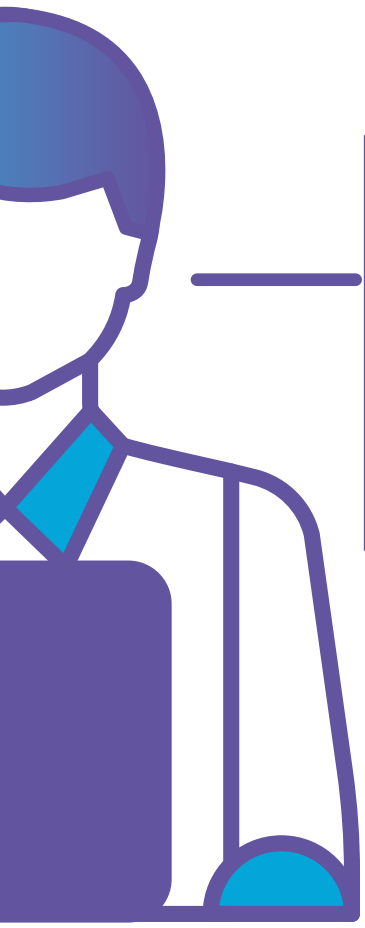
COMMENT CONTRIBUER À LA SÉCURITÉ DE L'INFORMATION ET DES DONNÉES À CARACTÈRE PERSONNEL ? //



LES BONNES PRATIQUES À RESPECTER PAR L'AGENT

L'agent doit mettre en œuvre des bonnes pratiques en matière de sécurité de l'information et de sécurité des données à caractère personnel. Celles-ci sont illustrées à l'aide de ce graphique et décrites plus en détail dans la présente section.





VIDÉOCONFÉRENCES

APPELS TÉLÉPHONIQUES

MESSAGERIE ÉLECTRONIQUE

« CLEVER CLICKS »

« BRING YOUR OWN DEVICE »

DÉPLACEMENTS PROFESSIONNELS

SÉCURITÉ DES LOCAUX DE L'ADMINISTRATION

TÉLÉTRAVAIL

POLITIQUE DU BUREAU PROPRE ET DE L'ÉCRAN VERROUILLÉ (« CLEAN DESK POLICY »)

CONTACTER LES SERVICES COMPÉTENTS EN CAS DE QUESTIONS OU DE DOUTES

Les mots de passe

L'authentification par « noms d'utilisateur » et « mots de passe » est le moyen le plus simple et le moins coûteux pour contrôler un accès, notamment à un ordinateur ou une application, et pour prouver l'identité de l'utilisateur.

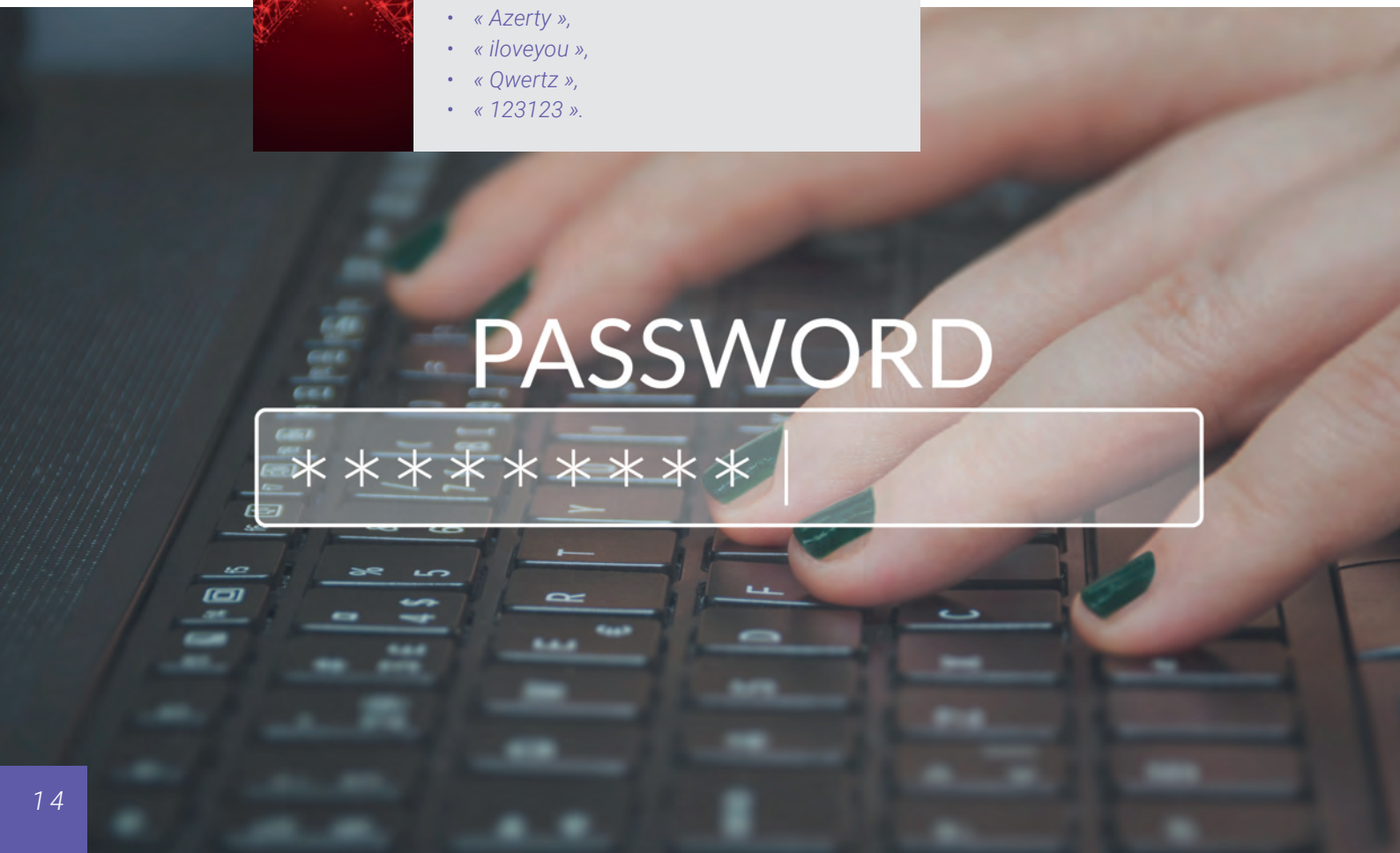
L'avantage de ce moyen d'authentification réside dans sa simplicité ainsi que dans le fait que la grande majorité des agents sont familiers avec cette mesure de sécurité.

Néanmoins, le recours aux mots de passe présente également des inconvénients :

- les mots de passe peuvent facilement être copiés ou observés à l'insu de l'utilisateur (ex. : attaques d'hameçonnage (« phishing ») ou regards par-dessus l'épaule des utilisateurs (« shoulder surfing »)) ;
- beaucoup d'utilisateurs emploient des mots de passe courants ou des mots de passe faciles à deviner (ex. : « 123456 », « Password » ou « QWERTY ») ;
- les individus utilisent un mot de passe unique pour plusieurs applications.

D'après les acteurs spécialisés en sécurité de l'information, figurent parmi les mots de passe les plus répandus :

- *« password »,*
- *« 123456 »,*
- *« 123456789 »,*
- *« Guest »,*
- *« QWERTY »,*
- *« abc123 »,*
- *« Azerty »,*
- *« iloveyou »,*
- *« Qwertz »,*
- *« 123123 ».*



Afin de minimiser les risques d'usurpation, il importe de choisir un mot de passe « fort » en respectant quelques règles essentielles :

1

Utiliser des mots de passe distincts pour des usages distincts.

L'**utilisation de mots de passe distincts** permet d'éviter les piratages en cascade. Ainsi, en cas de vol ou de perte du mot de passe, seule l'application ou seul le compte concerné sera vulnérable.

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI interdit la réutilisation de mots de passe personnels attachés à des comptes privés pour accéder aux systèmes d'information de l'Etat.

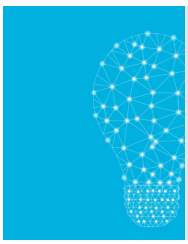
Utiliser un mot de passe suffisamment long et complexe, impossible à deviner.

2

Pour pouvoir résister à des attaques « force brute », le mot de passe doit être suffisamment long et complexe. D'après les bonnes pratiques actuelles, il doit être **composé d'au moins 12 caractères et comprendre à la fois des minuscules, des majuscules, des chiffres et des caractères spéciaux.**

L'attaque par « force brute » consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le mot de passe de l'utilisateur. Compte tenu des avancées techniques (utilisation de solutions d'intelligence artificielle), des dizaines de milliers de combinaisons par seconde peuvent être testées à l'occasion de ces attaques.

Par ailleurs, l'agent doit **éviter le recours aux mots du dictionnaire, aux suites logiques** (ex. : « 123456 » ou « QWERTZ ») **ainsi qu'aux informations personnelles** (ex. : le prénom de son enfant, son club de sport préféré, sa plaque d'immatriculation, sa date de naissance).



L'attaque par « dictionnaire » consiste à tester automatiquement tous les mots contenus dans les dictionnaires d'une langue donnée. Elle est basée sur l'hypothèse que l'agent a créé son mot de passe en utilisant un terme défini dans un tel dictionnaire. Compte tenu de l'avancement des technologies, ce type d'attaque permet de démasquer un mot de passe en quelques secondes.

Pour ces motifs, il est recommandé à l'agent de choisir son mot de passe en utilisant la technique de la « phrase » (« méthode des premières lettres ») ou la technique « phonétique », tout en respectant les conditions des caractères spéciaux (ex. : « @ », « ! » ou « & »), des chiffres, des minuscules ainsi que des majuscules.

Exemple d'un mot de passe par la technique de la « phrase » :

- *phrase à retenir : « deux vaches et un cheval sur le toit se posent trois questions »,*
- *mot de passe : « 2V&1Csltsp3? ».*

Exemple d'un mot de passe par la technique « phonétique » :

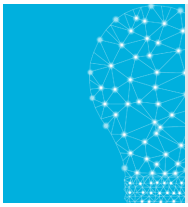
- *phrase à retenir : « : j'ai acheté huit cd pour cent euros cet après-midi »,*
- *mot de passe : « Ght8CD%E7ami ».*

3

Ne pas partager un mot de passe et ne pas le divulguer à des tiers.

Le mot de passe **doit rester secret** en toute circonstance. Ainsi, l'agent ne doit jamais :

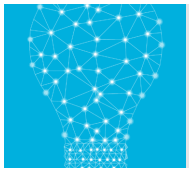
- demander à un tiers de générer son mot de passe ;
- partager son mot de passe avec d'autres personnes, y compris dans le cadre d'une utilisation commune de la même application informatique ;
- conserver son mot de passe en clair, que ce soit sous format électronique ou papier (ex. : mention du mot de passe sur un post-it collé sur l'écran, annotation du mot de passe au dos du clavier, envoi à soi-même du mot de passe par mail) ;
- divulguer son mot de passe à des tiers.



Ni le CTIE, ni le GOVCERT, ni le RSSI ou le DPD de l'administration ne demanderont à l'agent de communiquer le mot de passe par mail ou par téléphone. De ce fait, l'agent ne doit pas répondre à de telles demandes, car il s'agirait probablement d'une tentative d'extorsion de mot de passe.

Changer son mot de passe régulièrement.

L'agent doit changer son mot de passe régulièrement afin de réduire les risques de piratage.



A cette fin, le CTIE envoie à intervalles réguliers des messages informant les agents que leur mot de passe actuel arrivera à expiration au terme du délai communiqué et les invite à le renouveler.

Dans ce même ordre d'idées, l'utilisateur doit changer son mot de passe au moment de la première connexion lorsque celui-ci a été généré par défaut par le gestionnaire des équipements et des solutions informatiques.

Toutefois, pour que le changement du mot de passe à une fréquence régulière constitue une mesure réellement efficace, il convient de ne pas seulement modifier légèrement le mot de passe précédent, notamment en ajoutant ou modifiant un chiffre à la fin. A défaut, les bénéfices du changement de mot de passe en termes de sécurité seraient mineurs.

Changer son mot de passe immédiatement en cas de compromission réelle ou suspectée.

Dans l'hypothèse où l'agent suspecte une compromission de son mot de passe, il doit le changer immédiatement afin d'éviter des utilisations illicites par des tiers (sans préjudice de l'obligation d'alerter au plus tôt les services compétents).

Ne pas utiliser de gestionnaire de mots de passe sur Internet.

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI interdit l'utilisation de gestionnaires de mots de passe sur Internet, tout en recommandant, en cas de besoin, l'utilisation d'un coffre-fort numérique (ex. : Keepass) pour le stockage sécurisé et chiffré des mots de passe.

Ne pas laisser son navigateur ou une application mémoriser le mot de passe.

De nombreux logiciels, dont les navigateurs, offrent la possibilité de sauvegarder les mots de passe des utilisateurs afin de ne plus devoir les saisir. Malgré son aspect pratique, cette option emporte des risques substantiels en termes de sécurité de l'information.

Pour ces motifs, la Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI n'autorise pas la mémorisation de mots de passe dans les navigateurs Internet, mais recommande l'utilisation d'un coffre-fort numérique.

Ne pas tenter de contourner les systèmes d'authentification et d'accéder à des systèmes d'information avec les identifiants d'un autre utilisateur.

Il est interdit à l'agent d'essayer de contourner les systèmes d'authentification et d'accéder à des systèmes d'information avec les identifiants d'un autre utilisateur. De tels actes risquent de compromettre la sécurité des systèmes d'information et des données et d'exposer l'agent à d'éventuelles sanctions disciplinaires voire, le cas échéant, pénales.

L'authentification forte

Les méthodes d'authentification à plusieurs facteurs (« authentification forte ») offrent une protection renforcée par rapport à la méthode d'authentification par mot de passe.

L'authentification forte consiste en l'**utilisation d'au moins deux facteurs d'authentification** distincts, correspondant, en particulier :

À DES INFORMATIONS CONNUES PAR L'UTILISATEUR (EX. : MOT DE PASSE OU CODE PIN)

À UN OBJET QUE L'UTILISATEUR POSSÈDE (EX. : « SMARTCARD LUXTRUST »)

À UN ÉLÉMENT SPÉCIFIQUE DE L'UTILISATEUR (EX. : EMPREINTE DIGITALE OU RECONNAISSANCE FACIALE)

La multiplicité des facteurs d'authentification assure qu'un tiers ne puisse accéder au compte d'utilisateur dans l'hypothèse où il parviendrait à se procurer le mot de passe de l'agent, faute de disposer du second facteur d'authentification. Bien que l'utilisation de l'authentification forte n'empêche pas tous les types d'attaques, elle rend plus difficile le piratage du compte de l'agent.

Pour que cette mesure soit efficace, l'agent doit veiller à ne pas divulguer ses identifiants et respecter les bonnes pratiques applicables en la matière.

Dans le cadre de l'utilisation de la « SmartCard Luxtrust » (moyen d'authentification forte le plus courant dans les administrations étatiques et communales), il faut, en particulier :

- *choisir un code PIN complexe et non devinable,*
- *ne pas conserver son code PIN ensemble avec la SmartCard,*
- *ne pas partager son code PIN ou sa SmartCard avec un tiers,*
- *ne pas laisser la SmartCard dans le lecteur de carte de son ordinateur après utilisation.*

Le « Bring your own device »

La notion de « Bring your own device », aussi connue sous l'acronyme « BYOD », décrit la situation dans laquelle les agents apportent leur matériel personnel (ex. : téléphone, tablette) dans l'environnement professionnel et l'utilisent tant à des fins privées qu'à des fins professionnelles.

Le phénomène du BYOD, bien que constituant une ouverture pratique pour l'utilisateur, comporte des risques en termes de sécurité de l'information, notamment dû au fait que les équipements privés risquent de ne pas être protégés de manière aussi sécurisée que les ressources informatiques gérées par les administrations.

Pour cette raison, **l'utilisation du BYOD est strictement encadrée par le CTIE**, à savoir notamment par la Charte d'accès à la messagerie de l'Etat avec un équipement mobile privé (BYOD) et le Guide des bonnes pratiques en matière de la sécurité d'information mobile.

En outre, l'accès au réseau de l'Etat est réservé aux équipements autorisés, gérés et mis à disposition par les services compétents. La connexion d'équipements privés ou d'équipements visiteurs, qu'elle soit filaire ou sans fil, au réseau de l'Etat est interdite. Cette restriction ne s'applique évidemment pas aux réseaux dédiés à la connexion de terminaux personnels ou visiteurs.

A noter que l'agent doit en tout état de cause s'abstenir de prendre en photo ou vidéo des documents ou des informations professionnels non publics avec ses équipements privés (ex. : smartphone). De même, il lui est interdit d'enregistrer les paroles d'autrui, à moins d'avoir obtenu le consentement préalable des personnes concernées ou d'être habilité par ou en vertu de la loi.

Le réseau privé virtuel (« VPN »)

L'usage du VPN permet aux agents de travailler en dehors des locaux de l'administration tout en accédant de manière sécurisée au réseau interne de celle-ci.

Un VPN est un moyen de communication assurant la sécurité des transferts de données sur des réseaux publics ou partagés. Il s'agit d'une technologie permettant l'extension logique du réseau, par l'ajout de postes ou sous-réseaux se trouvant à l'extérieur des limites physiques de celui-ci. Grâce à des mécanismes cryptographiques, le canal VPN s'apparente à un tunnel virtuel ne contenant que des données chiffrées non-modifiables.

Compte tenu du fait que l'accès à distance aux ressources informatiques internes de l'Etat et des communes est réservé aux personnes ayant le besoin métier, l'agent travaillant à distance et se connectant à des ressources informatiques pour des besoins professionnels doit :

- disposer d'une autorisation formelle de sa hiérarchie ;
- n'utiliser que le matériel fourni, à savoir un moyen de connexion spécifiquement configuré à ces fins et sécurisé ;
- veiller à ce que le matériel fourni pour le télétravail ou l'accès à distance ne soit pas utilisé par un tiers ;
- ne pas contourner ou tenter de contourner les mesures et dispositifs de sécurité permettant d'assurer une connexion sécurisée à distance.

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI rappelle que chaque utilisateur accédant au VPN de l'Etat est personnellement responsable de l'utilisation qu'il en fait.

Les réseaux sans-fil (Wifi)

L'agent doit veiller à ce que la connexion au réseau sans-fil (« Wifi ») ne nuise pas à la sécurité de l'information de l'administration.

De ce fait, il doit dans le cadre de ses activités professionnelles éviter au maximum l'utilisation de réseaux Wifi non gérés par l'administration.

Par ailleurs, en cas de connexion à un réseau Wifi à des fins professionnelles, l'agent doit :

- n'activer l'interface Wifi que lorsque celle-ci doit être utilisée,
- éviter de se connecter à des réseaux sans-fil non sécurisés (ex. : Wifi d'hôtel, de gare ou de café),
- recourir aux solutions VPN prévues par le gestionnaire informatique,
- s'assurer que le pare-feu et l'antivirus sont activés,
- choisir une authentification forte lors d'une connexion à une application,
- désactiver le réseau sans-fil à la fin de l'utilisation,
- désactiver la connexion automatique aux points d'accès Wifi déjà utilisés.

Les exigences relatives à la connexion Wifi s'appliquent également lors de l'utilisation d'un réseau filaire inconnu ou non sécurisé (branchement au câble « Ethernet »).

L'agent doit également s'abstenir de consulter tout site Internet à risque pour la sécurité de l'information, notamment en termes d'intrusion dans les systèmes (ex. : exécution de virus, prise de contrôle à distance).

Les acteurs spécialisés en la matière, tel que le CTIE, restreignent l'accès à certains sites Internet à risque.

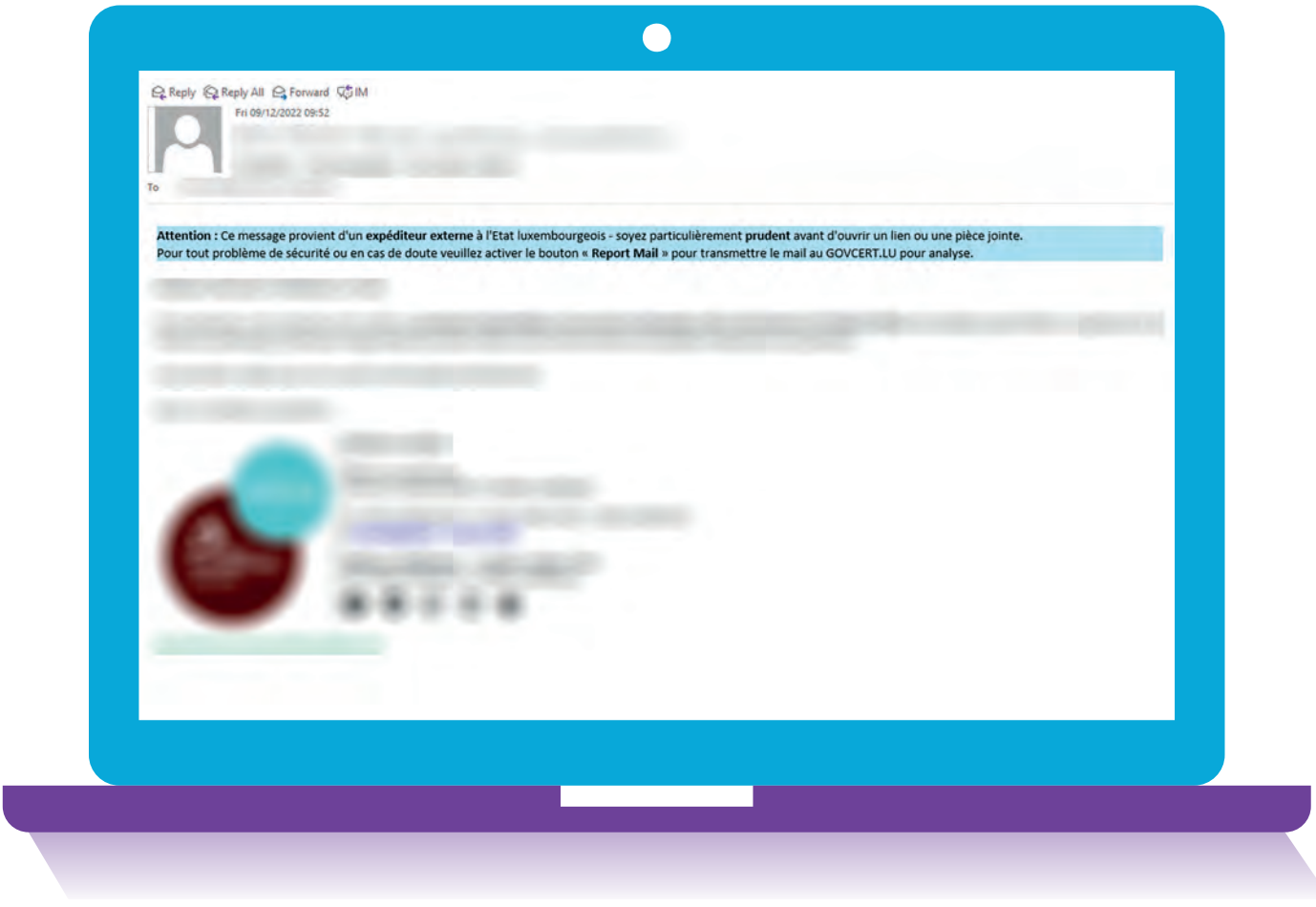
La messagerie électronique

Le mail est la principale forme de communication professionnelle de l'agent. Son utilisation nécessite une vigilance accrue de l'agent, tant au niveau de l'expédition que de la réception d'un message.

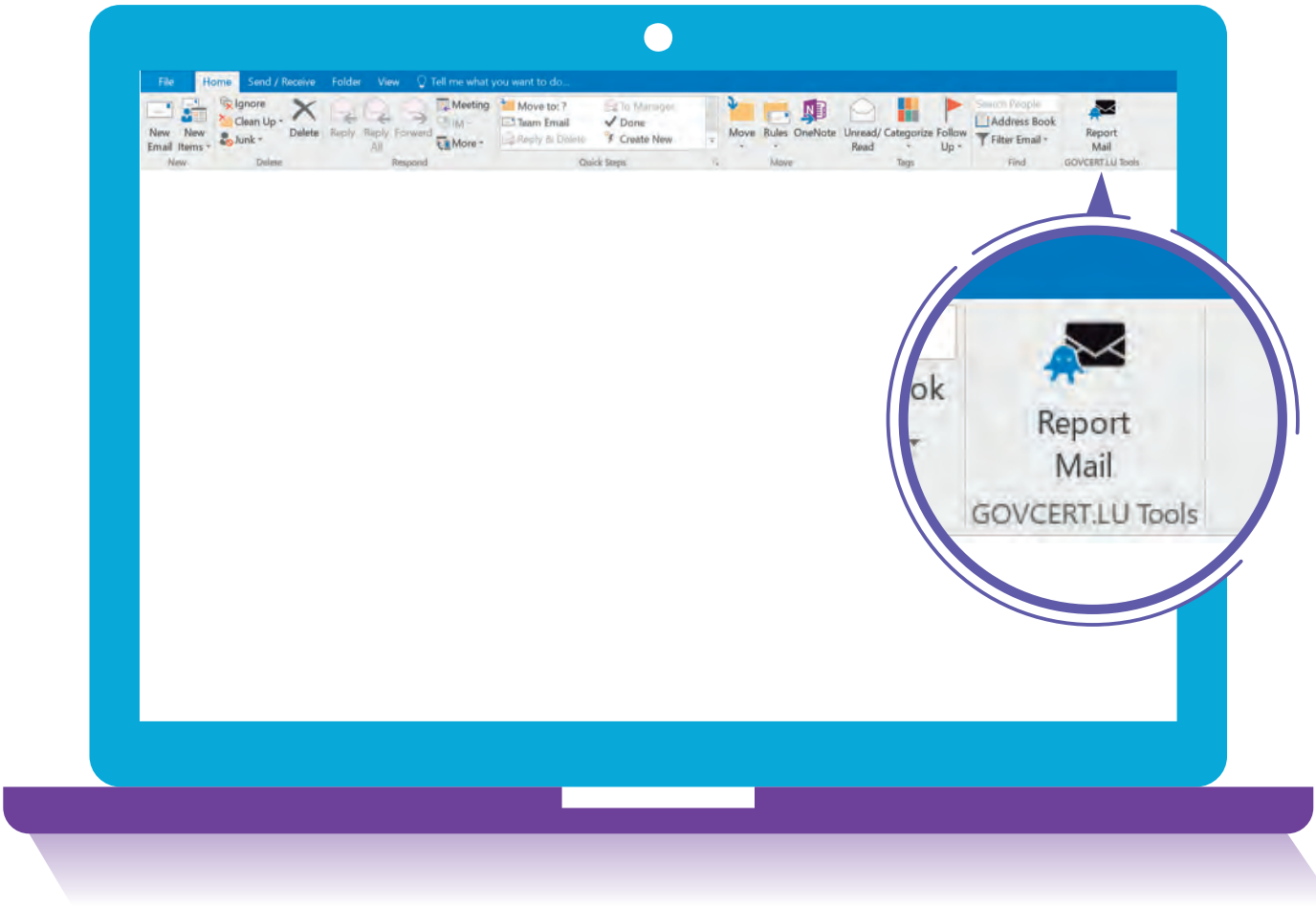
Pour ces raisons, l'agent doit, en particulier :

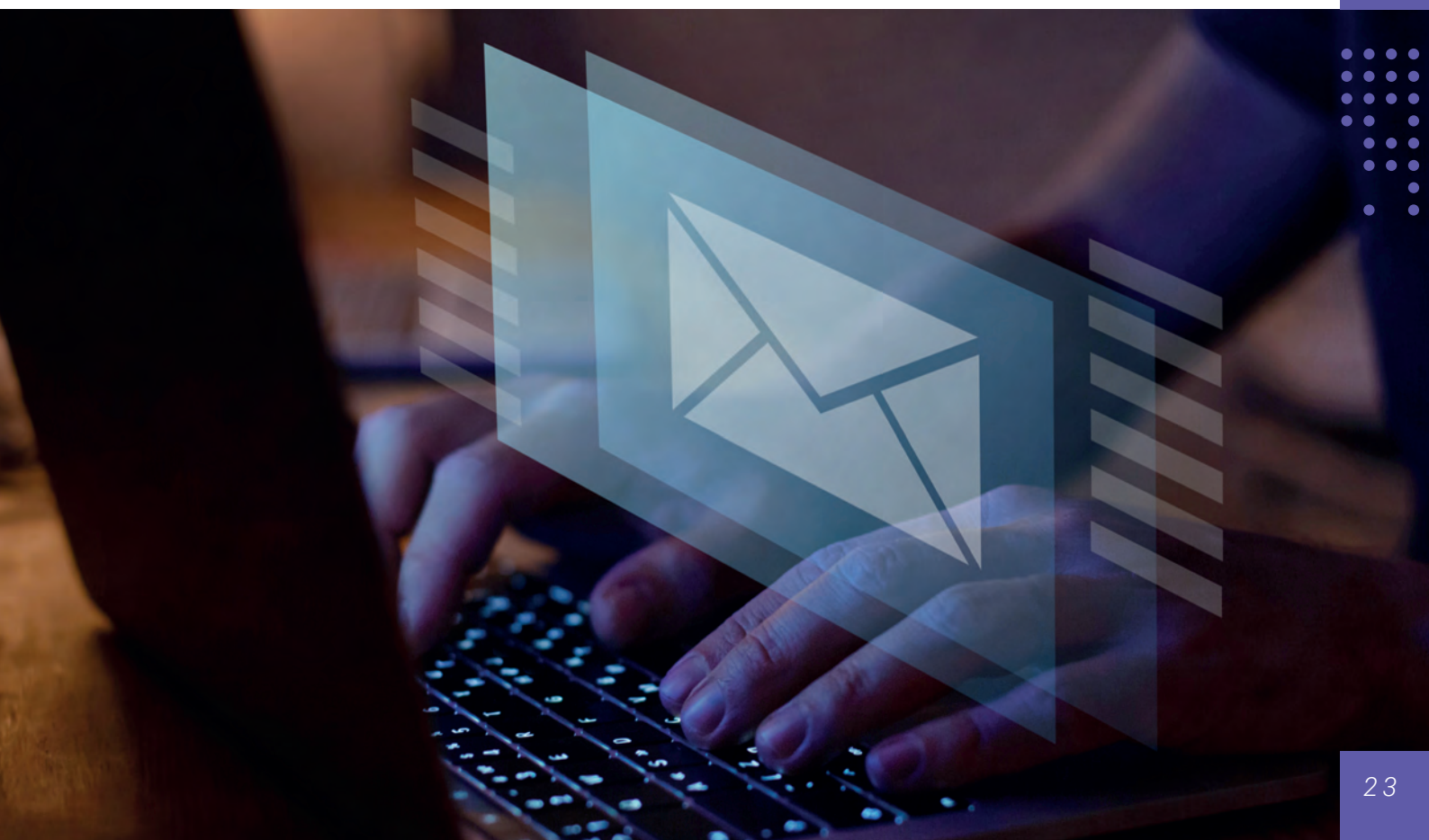
- être conscient du fait que l'acheminement, l'authenticité et l'intégrité des messages véhiculés par Internet ne sont pas garantis. Il doit faire preuve de vigilance lorsqu'il reçoit un mail avec une pièce-jointe ou contenant un lien vers un site Internet, surtout si celui-ci est de provenance inconnue ou douteuse.

Le CTIE a inséré une bannière d'information dans les mails en provenance de sources non-étatiques. L'objectif étant d'attirer l'attention des agents sur le risque qu'un tel mail externe puisse être potentiellement frauduleux et sur la nécessité, pour l'agent, de le traiter avec les précautions nécessaires.

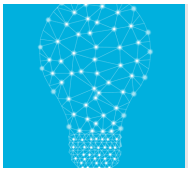


- transmettre au GOVCERT les mails suspicieux (ex. : soupçon d'attaque « phishing ») en utilisant la fonction « Report Mail » dans sa messagerie électronique.





- s'abstenir de transférer des mails ou documents professionnels vers des adresses mails privées, qu'il s'agisse de la sienne ou celles de tiers non autorisés (ex. : membre de sa famille).



Cette interdiction vise par exemple le transfert de documents professionnels vers une adresse mail privée à des fins d'impression de documents en télétravail en ayant recours au matériel informatique privé.

- recourir à des moyens de chiffrement adéquats, fournis par le gestionnaire informatique de l'administration, en cas de transmission d'informations confidentielles.

Exemple :

L'application « One-Time-Exchange » (« OTX ») permet à un agent d'échanger des fichiers électroniques avec des personnes tierces via un canal sécurisé. La notification d'un envoi de fichier ou d'une demande de fichiers est transmise par mail. L'agent peut ensuite accéder aux documents via l'application Web OTX. Le fichier transmis reste disponible pour le destinataire durant une période définie.

- s'assurer de la confidentialité des données communiquées par mail en vérifiant notamment la légitimité des destinataires et des pièces jointes. En effet, une simple erreur ou négligence peut conduire au transfert de données à des tiers non habilités et partant à un incident de sécurité de l'information.

Dans certains cas de figure, l'envoi de messages groupés à plusieurs destinataires doit se faire sans divulguer les adresses mail des destinataires (ex. : en utilisant la fonction « Cci »). Il convient également de s'assurer que chaque destinataire est bien autorisé à recevoir les informations contenues dans le mail.

- s'abstenir d'utiliser sa boîte mail comme un espace de stockage, en particulier pour les données qui peuvent paraître sensibles (ex. : les fiches de rémunération).

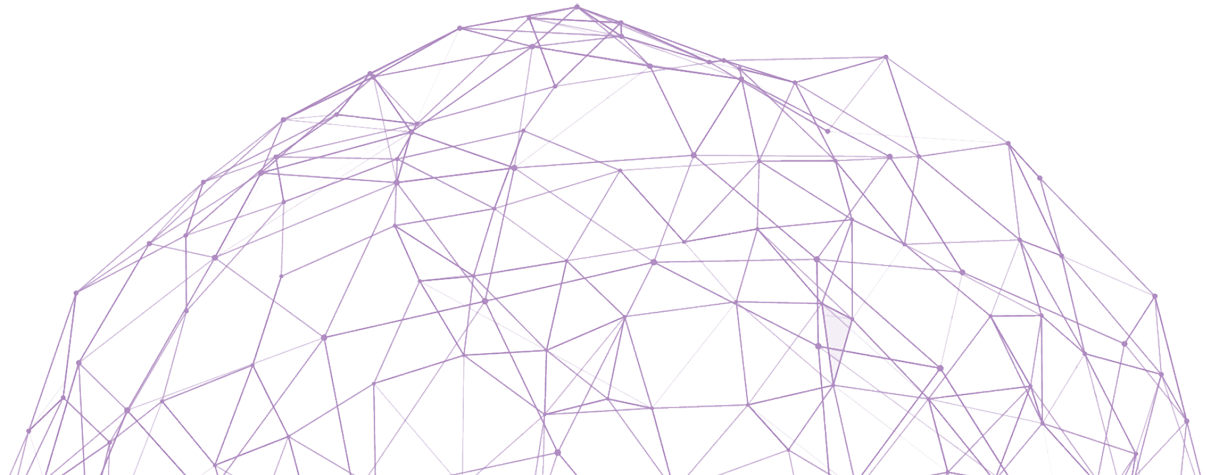
Les réseaux sociaux

L'agent ne doit pas partager des informations professionnelles non publiques via les réseaux sociaux, les applications et les services de messageries instantanées qui ne sont pas gérés par l'administration publique (ex. : Facebook, Twitter, Instagram,TikTok, WhatsApp).

Compte tenu du fait que ces outils ne sont pas contrôlés par les administrations, leur installation et utilisation sur les équipements professionnels comportent des risques en termes de sécurité de l'information et de partages illicites de données avec des tiers. De ce fait, elles sont déconseillées. En tout état de cause, une utilisation de services en ligne commerciaux non contrôlés par l'administration publique ne doit se faire qu'avec précaution et retenue.

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI précise que l'utilisation des réseaux sociaux doit se faire selon les règles de bonne conduite et d'éthique.

L'agent doit être conscient des risques associés à l'utilisation de ces services et s'abstenir, en particulier, de publier des informations professionnelles non publiques via ces canaux.



Les déplacements professionnels

Dans le cadre de ses fonctions, l'agent peut être amené à effectuer des déplacements professionnels. Il devra alors faire preuve d'une vigilance accrue notamment quant aux équipements informatiques et aux informations professionnelles qu'il transporte en dehors des locaux de l'administration.

L'agent doit s'assurer, en particulier, des points suivants :

Avant le déplacement :

- prévoir d'accéder aux informations à distance de façon sécurisée (ex. : par le biais d'un site sécurisé ou d'un VPN) ;
- n'emporter que les informations nécessaires à l'accomplissement de sa mission ;
- s'assurer que les données emportées sont sauvegardées sur un support conservé au sein de l'administration ;
- protéger adéquatement les informations confidentielles emportées (ex. : utilisation de supports de stockage chiffrés).

Au cours du déplacement :

- conserver et transporter les équipements et les informations de manière sécurisée (ex. : ne pas laisser l'ordinateur portable de manière visible dans une voiture ou sans surveillance dans un espace public) ;
- faire preuve de discrétion et ne pas consulter des documents professionnels en présence de personnes non autorisées (ex. : ne pas discuter à haute voix de dossiers professionnels en présence de tiers non autorisés, notamment au cours de déplacements en train ou avion) ;
- éviter la connexion à des réseaux, des systèmes informatiques et des équipements non sécurisés ;
- prévenir au plus vite ses supérieurs hiérarchiques et les services compétents (ex. : CTIE, GOVCERT, le RSSI de l'administration et le DPD) en cas de perte ou de vol de matériels ou d'informations.

Après le déplacement :

- détruire les documents dont l'administration n'a plus besoin (sans préjudice des dispositions de la loi du 17 août 2018 relative à l'archivage) ;
- faire vérifier, par les services compétents, les équipements utilisés lors du déplacement en cas de doute sur leur intégrité.

A noter que l'agent reste tenu par ses obligations statutaires et légales, ainsi qu'à son obligation de confidentialité dans le cadre de déplacements professionnels.

La destruction de documents

L'agent doit garantir la confidentialité des données ainsi que des documents et informations professionnels non publics pendant tout leur cycle de vie.

De ce fait, leur destruction doit se faire de manière sécurisée, quel que soit leur support (électronique ou papier). Ainsi, il est interdit à l'agent de jeter des documents confidentiels ou contenant des données dans les poubelles ordinaires.

En revanche, l'agent doit détruire ces documents à l'aide de déchiqueteuses, à moins que des procédures mises en place par l'administration prévoient des procédures plus strictes (ex. : le recours à des poubelles sécurisées fournies par des prestataires certifiés procédant à une destruction irréversible).

Le service des imprimés et fournitures de bureau (« IFB ») du CTIE peut être mandaté par les administrations pour la destruction de leurs documents (mise à disposition de bacs pour l'enlèvement de documents obsolètes avec destructions des données confidentielles).

A noter que la destruction doit se faire dans le respect des dispositions de la loi du 17 août 2018 relative à l'archivage et des engagements pris par l'administration dans le tableau de tri cosigné avec les Archives nationales.

Les mises à jour

Les équipements informatiques, les solutions techniques et les logiciels fournis par l'administration doivent être mis à jour **dans les meilleurs délais.**

Bien que les processus de mise à jour puissent être ressentis comme une contrainte, notamment lorsqu'ils interrompent une activité professionnelle, **l'agent ne doit pas retarder les mises à jour** ou ignorer les messages indiquant leur disponibilité.

Les services compétents pour la gestion de ces dispositifs (ex. : le CTIE), définissent les règles et processus de mises à jour. Elles sont ensuite portées à l'attention de l'agent.

Les vidéoconférences

Les outils de vidéoconférence font partie des outils indispensables à disposition des agents, en particulier dans le contexte du télétravail.

Le recours à ce type d'outil présente toutefois des risques en termes de sécurité de l'information. La mauvaise utilisation ou le paramétrage erroné des systèmes ainsi que l'existence de failles logicielles peuvent compromettre les données (ex. : écoute non autorisée de discussions, prise de contrôle de la caméra de participants). Par ailleurs, le partage de documents contenant des informations sensibles via une plateforme de vidéoconférence non gérée par les administrations publiques peut avoir pour conséquence que les informations transitent sur des serveurs non maîtrisés.

Afin de se prémunir contre ces conséquences dommageables, l'agent doit notamment :

- recourir à des plateformes de vidéoconférence gérées ou recommandées par les administrations publiques, telles que le CTIE ;
- s'assurer que seules les personnes habilitées participent à la vidéoconférence, notamment en restant attentif aux nouvelles connexions et à la liste des participants au cours de la réunion ;
- utiliser, si possible, la fonction « salle d'attente » pour filtrer les participants à la réunion, notamment lorsque la plateforme ne permet pas de restreindre l'accès par mot de passe ;
- ne pas enregistrer les vidéoconférences, à moins d'avoir préalablement recueilli le consentement des personnes concernées ou d'y être autorisé par ou en vertu de la loi ;
- éviter tout partage d'écran indésirable ;
- à la fin de la vidéoconférence, s'assurer de fermer la session en cours.

La loi du 11 août 1982 concernant la protection de la vie privée prévoit que toute atteinte volontaire à la vie privée d'autrui en écoutant ou en enregistrant, au moyen d'un appareil quelconque, des paroles prononcées en privé ou en observant une personne dans un lieu non accessible au public, sans le consentement de celle-ci, est sanctionnée pénalement.

La politique du bureau propre et de l'écran verrouillé (« Clean desk policy »)

Afin de réduire les risques d'accès non autorisé, de perte et d'endommagement d'informations confidentielles et de données, l'agent doit mettre en œuvre une politique de bureau propre et d'écran verrouillé, chaque fois qu'il s'absente de son poste de travail.

Dans ce contexte, il doit notamment :

- ranger son espace de travail lorsqu'il quitte son poste de travail ou lorsqu'il reçoit un visiteur dans son bureau et conserver les documents papiers de manière sécurisée (ex. : armoires de bureau fermées à clé) ;
- ne pas laisser sans supervision des documents confidentiels dans l'imprimante, la photocopieuse, ou sur le bureau ou tout autre endroit potentiellement exposé ;
- ne pas conserver des documents et des données dans des lieux accessibles à des personnes non autorisées ;
- mettre son ordinateur en mode veille, en cas d'absence prolongée, et l'éteindre en dehors des heures de bureau.

Le besoin d'en connaître (« need to know »)

L'agent doit traiter les données dans les strictes limites des missions d'intérêt public poursuivies par l'administration et pour les seuls objectifs fixés par celle-ci dans le cadre de ses attributions.

Tout détournement et toute communication à des tiers contraires aux lois et règlements sont interdits.

La consultation à des fins privées de données contenues dans un fichier tenu par l'administration, tel que le registre national des personnes physiques (RNPP), constitue un détournement de finalité strictement interdit par la loi. Il en va de même pour les consultations à des fins privées, par les agents communaux, notamment du registre d'état civil.

L'agent ne doit pas transmettre ou divulguer des données à un destinataire (interne ou externe à l'administration) qui ne remplit pas, au moment de la réception des données, les conditions dans lesquelles il est habilité à les traiter.

En outre, il doit informer son supérieur hiérarchique dans les meilleurs délais lorsqu'il constate qu'il dispose d'accès indus (ex. : des droits qui n'auraient pas été supprimés après un changement d'affectation).

La sécurité des locaux de l'administration

L'agent doit respecter les mesures de sécurité physiques mises en place par l'administration et ne pas tenter de les contourner. Il ne doit, en particulier, pas :

- empêcher la fermeture d'une porte d'entrée contrôlée, que ce soit par courtoisie (ex. : tenir la porte ouverte à des personnes inconnues) ou par facilité (ex. : bloquer la porte d'entrée durant l'intervention d'un technicien) ;
- prêter son badge à autrui ;
- permettre à une personne d'accéder à une zone contrôlée sans que celle-ci ne se soit conformée aux procédures préalables de vérification existantes (ex. : protocole d'accueil des visiteurs) ;
- laisser un visiteur circuler sans surveillance dans les locaux de l'administration.

Au contraire, il doit contribuer à la sécurité des locaux de l'administration en restant vigilant et en signalant sans délai à ses supérieurs hiérarchiques toute suspicion de présence d'une personne non autorisée.

Les appels téléphoniques

L'agent doit veiller à ne pas divulguer des informations confidentielles à des personnes non habilitées ou malveillantes à travers le canal de communication des appels téléphoniques.

Pour ne pas communiquer de données à des personnes non autorisées, l'agent doit en particulier :

- vérifier l'identité de l'interlocuteur en lui demandant des informations précises (ex. : nom, prénom ainsi que matricule, couplés à des informations appropriées en fonction du contexte telles que le numéro de dossier) ;
- s'interroger sur la crédibilité d'une demande en tenant compte des éléments factuels ;
- vérifier, le cas échéant, les informations fournies par l'interlocuteur (ex. : en contactant l'organisation citée via des coordonnées publiques ou précédemment connues).

Le télétravail

Le télétravail permet à un agent de réaliser son activité professionnelle en dehors de son lieu de travail habituel.

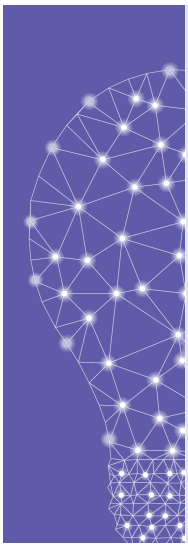
L'agent doit utiliser les équipements et accès professionnels de manière responsable et vigilante quand il travaille à distance. Ainsi, il est notamment tenu :

- d'appliquer rigoureusement les politiques et standards de sécurité mis en place par l'administration (ex. : respect de la Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI). Dans ce contexte, il reste soumis aux mêmes obligations que l'utilisateur travaillant sur site ;
- de s'abstenir de connecter ses équipements professionnels à des réseaux publics non maîtrisés ou non sécurisés ;
- de sécuriser le réseau domestique utilisé par un paramétrage approprié (ex. : routeur privé de connexion Internet sécurisé par mot de passe) ;
- d'utiliser le réseau VPN mis à disposition par l'administration ou le cas échéant par le gestionnaire informatique ;
- d'utiliser les équipements et outils informatiques de manière responsable (ex. : séparer les usages privés des usages professionnels) ;
- de rester vigilant quant aux tentatives d'attaques informatiques (ex. : attaque phishing, ingénierie sociale).

L'agent en télétravail est également tenu de prévoir un espace dédié à ses activités professionnelles qui garantit la confidentialité des informations qu'il traite. Pendant les heures de travail, cet espace ne doit pas être accessible à des tiers (ex. : membres de la famille). En effet, il convient de veiller à ce que les discussions professionnelles restent confidentielles, en particulier lors de l'utilisation d'outils de vidéoconférence à domicile, et de s'assurer à ce qu'aucun tiers n'accède aux informations que l'agent traite dans le cadre de l'exercice de ses fonctions.

Les « Clever clicks »

Un danger répandu de la sécurité de l'information consiste à inciter l'utilisateur à cliquer sur un lien suspect placé dans un mail (ex. : attaque phishing), à télécharger un logiciel malveillant (ex. : cheval de Troie) ou à utiliser des QR-Codes qui mènent à des sites corrompus. Pour s'en prémunir, **l'agent doit éviter de cliquer de manière imprudente sur des liens ou des applications** (« clever clicks »).



L'agent peut éviter de nombreux problèmes de sécurité de l'information en respectant notamment les bonnes pratiques suivantes :

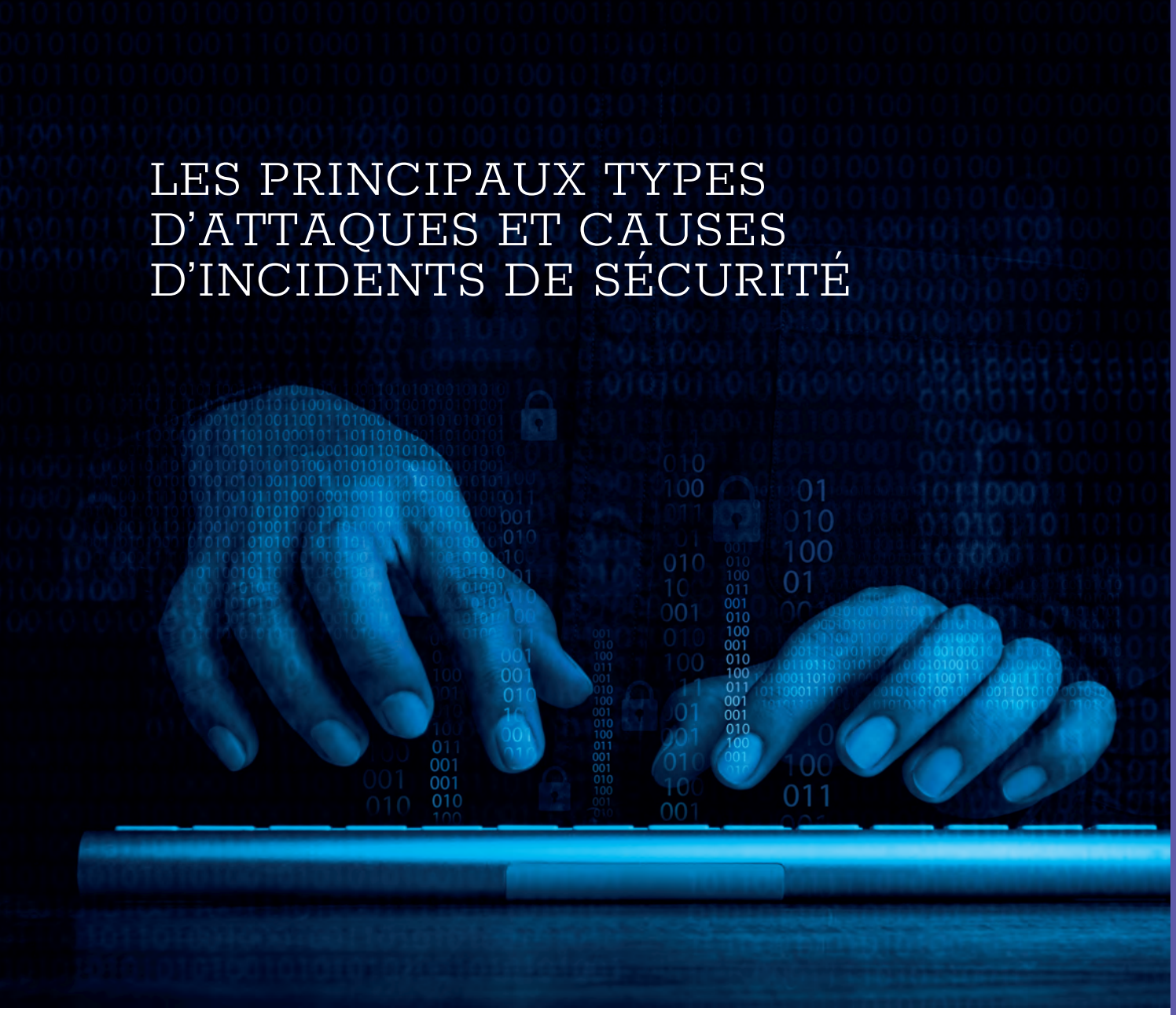
- *ne télécharger de logiciels qu'à partir des sources vérifiées par l'administration publique, en particulier le CTIE ou le gestionnaire du réseau informatique ;*
- *en cas de doute par rapport à un lien contenu dans un mail, ne pas cliquer dessus sans avoir eu au préalable la confirmation par les organes compétents (ex. : le GOVCERT) de son caractère non nuisible ;*
- *ne pas « couper ou copier » un lien suspect se trouvant dans un mail ou SMS pour ensuite le « coller » dans son navigateur ;*
- *faire preuve de prudence face à tout type de pièce jointe dans un système de messagerie, même si elle provient d'un expéditeur connu ;*
- *se déconnecter correctement de son accès lorsque l'on quitte une application ;*
- *ne pas répondre à un message frauduleux, mais le signaler au service compétent.*

Ainsi, l'agent doit faire preuve d'une prudence accrue lors de la navigation sur Internet dans le cadre de ses activités professionnelles.

Contacter les services compétents en cas de questions ou de doutes

En cas de doutes, de suspicions d'une attaque ou d'un risque pour la sécurité de l'information, l'agent doit contacter son supérieur hiérarchique ainsi que les services de sécurité de l'information compétents de son administration (ex. : le gestionnaire informatique, tel que le CTIE, le GOVCERT, le RSSI, si désigné par l'administration, et le DPD).

LES PRINCIPAUX TYPES D'ATTAQUES ET CAUSES D'INCIDENTS DE SÉCURITÉ



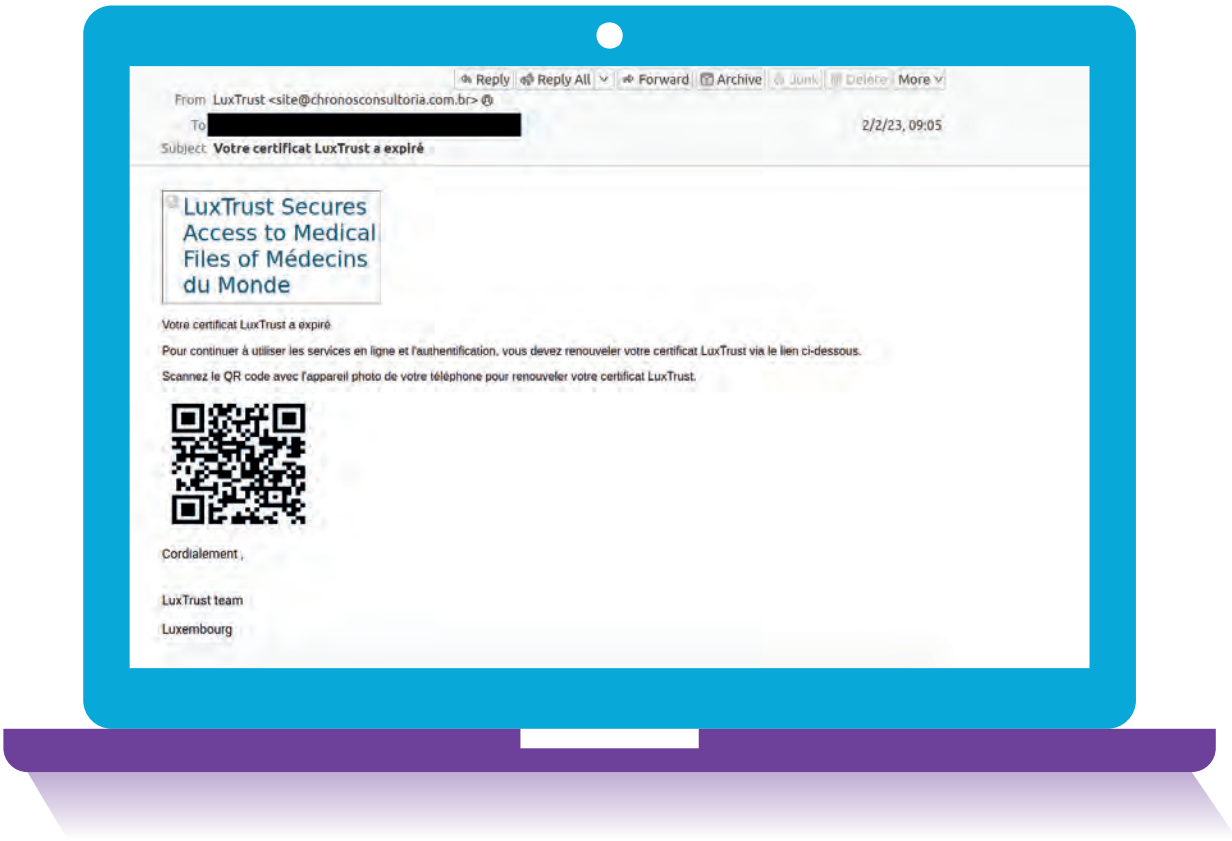
L' « hameçonnage » (« phishing »)

Le phishing est une forme d'escroquerie sur Internet employée par une personne malveillante pour récupérer des informations et des données traitées par un autre individu. L'attaquant se fait passer pour un organisme de confiance et incite ainsi la victime potentielle à l'ouverture d'une pièce-jointe malveillante, à l'accès à un site web contrefait ou à la communication de mots de passe ou d'informations confidentielles.

Pour ce faire, l'attaquant utilise le plus souvent le canal de la messagerie électronique en envoyant un mail reprenant la mise en page, le nom et le logo de l'entité dont il usurpe l'identité et en y intégrant la pièce jointe ou le lien frauduleux.

L'objectif de cette manœuvre est d'inciter l'agent, sous un faux prétexte, à se rendre sur un site web contrefait et à y introduire ses données (ex. : mise à jour d'un compte en ligne en cours d'expiration) ou à ouvrir une pièce jointe malveillante (ex. : contenant un virus).

Exemple d'un mail de « phishing » :



Bien que le but soit toujours le même, les attaques de phishing peuvent également prendre d'autres formes. Une méthode de phishing de plus en plus répandue consiste en l'envoi de SMS frauduleux renvoyant vers des sites Internet contrefaits.

Dans le cadre des campagnes de sensibilisation des agents étatiques, l'ANSSI rend attentif à l'existence d'attaques de type « phishing » par SMS (encore appelées « smishing ») s'appuyant sur la manipulation psychologique de la victime pour compromettre des systèmes d'information.

Très souvent, le message de « smishing » crée un sentiment d'urgence. Les messages peuvent contenir des mots ou phrases comme « action immédiate requise », « votre compte a été compromis » ou « vous vous exposez à des poursuites judiciaires si vous ne réagissez pas ».

Ces SMS frauduleux sont envoyés dans le but d'inciter le destinataire à ouvrir un lien transmis. L'utilisateur est ensuite invité à y saisir des informations personnelles, comme par exemple des coordonnées bancaires ou des données d'identification en ligne.

Les attaques de phishing peuvent avoir des **conséquences graves** pour la victime. Sur base des informations fournies par cette dernière, les attaquants vont pouvoir obtenir des avantages notamment :

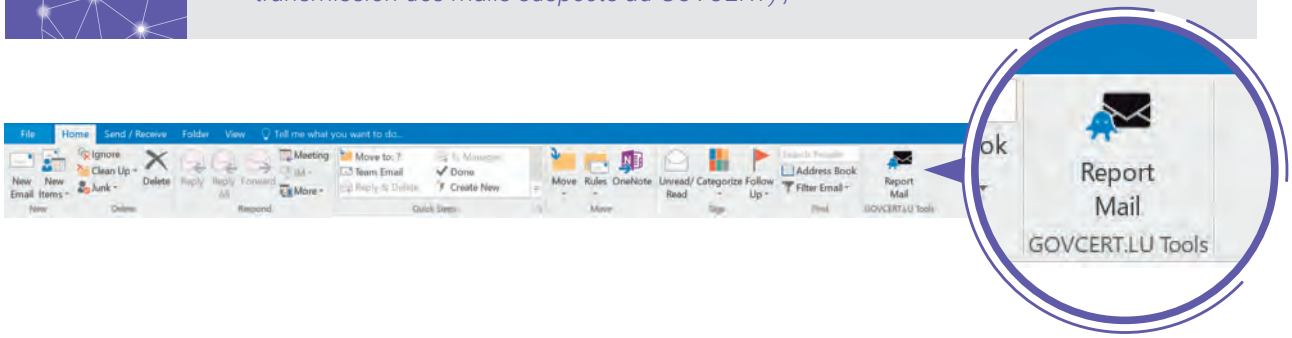
FINANCIERS (EX. : DÉTOURNEMENT D'ARGENT)

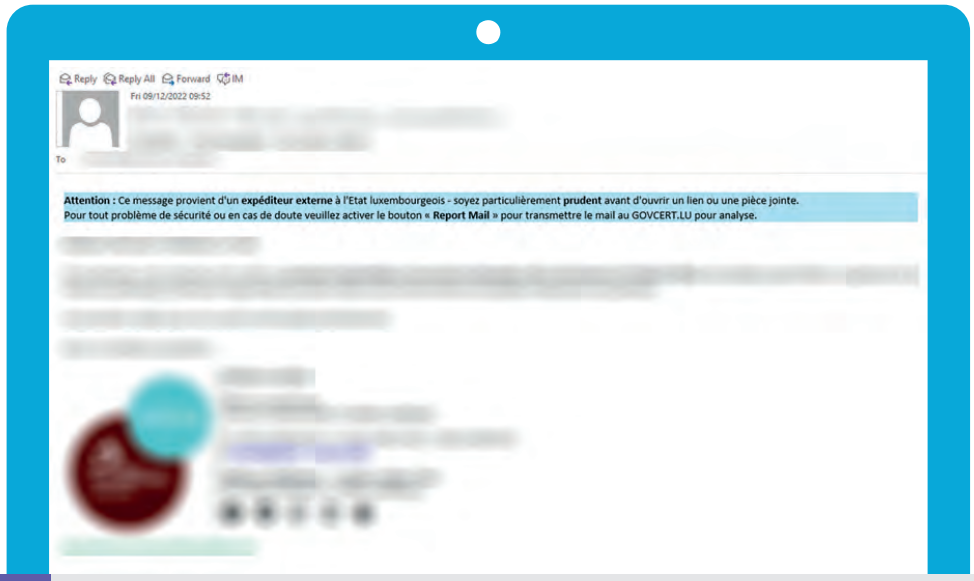
MATÉRIELS (EX. : ACCÈS AUX SYSTÈMES D'INFORMATION DE L'ADMINISTRATION)

MORAUX (EX. : EXERCICE DE PRESSION SUR LA VICTIME)

Les moyens de prévention :

- *transmettre immédiatement au GOVCERT les mails suspects. Pour ce faire, l'agent peut notamment utiliser la fonction « Report Mail » dans sa boite mail « Outlook ». Sur base de ce signalement, le GOVCERT informe l'agent du caractère malveillant ou non du mail (à noter que certaines entités ont prévu que leur RSSI soit le point de contact pour la transmission des mails suspects au GOVCERT) ;*





- *être particulièrement vigilant lorsque le message provient de l'extérieur (signalé par une bannière d'information du CTIE) ;*
- *contrôler si le message est personnellement adressé au destinataire ;*
- *vérifier la qualité rédactionnelle du message (ex. : fautes, traductions erronées, formules de politesse et de salutation inadaptées au contexte, signature du mail différente de la signature officielle, etc.) ;*
- *vérifier l'adresse d'expédition (ex. : annuaire public ou carnet d'adresses fiables), le cas échéant, en contactant l'expéditeur par un canal officiel et fiable pour s'assurer qu'il est bien à l'origine du message ;*
- *vérifier l'authenticité de l'adresse web (URL) du navigateur avant de s'authentifier.*

*Par ailleurs, il convient d'**être d'autant plus vigilant face à un mail qui porte sur une demande de communication d'informations personnelles** ou qui comporte des pièces jointes ou des liens externes.*

Le « spear phishing »

Les attaques de spear phishing sont une forme particulière de phishing qui s'appuient généralement sur des tactiques poussées d'ingénierie sociale.

Elles consistent, tout comme les attaques de phishing classiques, dans l'usurpation de l'identité numérique d'un tiers et visent à duper le destinataire en vue de l'inciter à ouvrir une pièce jointe ou un lien vers un site Internet malveillant. Toutefois, s'y ajoute un élément frauduleux supplémentaire, à savoir un ciblage très précis qui s'adresse au destinataire du message.

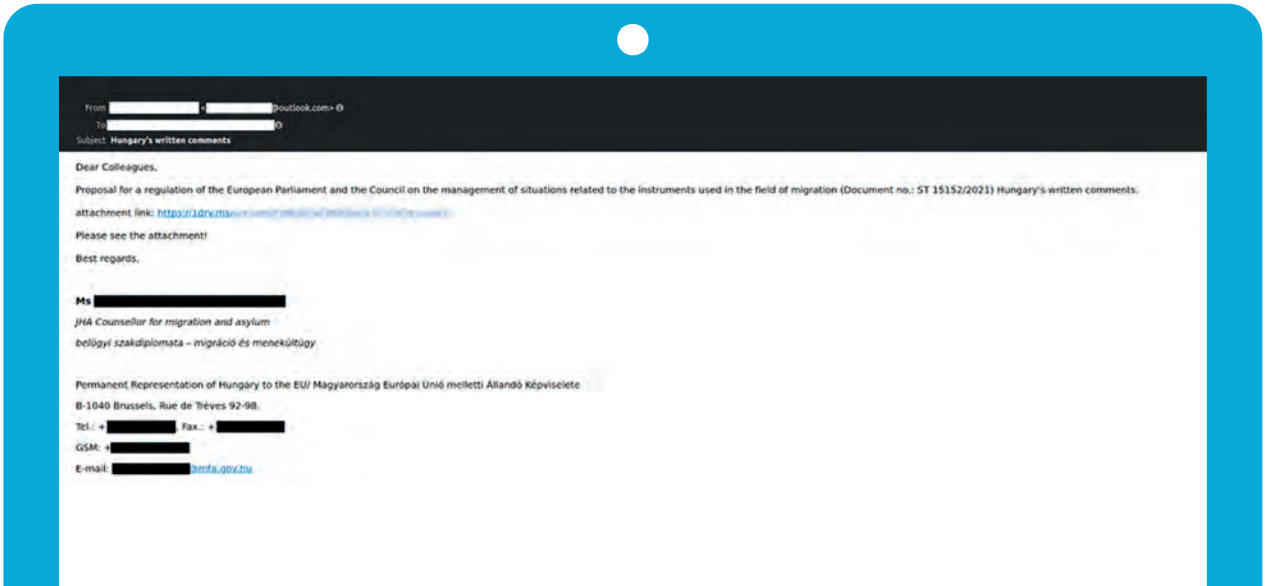
Ainsi, les attaques de type spear phishing sont plus élaborées, hautement personnalisées et minutieusement préparées avant leurs mises en œuvre.

Les moyens de prévention :

Quelques éléments suspects permettent d'identifier qu'il s'agit d'une attaque de spear phishing, notamment :

- *les attaques de spear phishing se caractérisent par l'usage d'un compte mail spécifiquement créé, typiquement sur une plateforme de messagerie publique (Outlook, Gmail, etc.), pour usurper l'identité d'un tiers (ex. : le mail est envoyé à partir d'une adresse Outlook sous la forme : firstname.lastname@outlook.com avec « first name » et « last name » étant le prénom et nom d'un agent usurpé) ;*
- *l'objet du mail est souvent lié à un sujet d'intérêt actuel pour susciter l'attention de la victime ciblée et l'inciter à l'ouvrir ;*
- *contrairement aux mails de type phishing, ceux de type spear phishing sont, en principe, mieux rédigés (pas ou peu de fautes de grammaire, brève explication sur le sujet, renvoi à un document contenant des informations supplémentaires, etc.) ;*
- *le lien (« hyperlink ») ajouté au mail de spear phishing peut être modifié quant à son apparence grâce à la fonctionnalité « modifier le lien hypertexte ». Ceci permet à l'attaquant d'induire sa victime en erreur en la dirigeant sur un site Internet malveillant paraissant tout à fait légitime (une lettre ou un caractère en trop ou en moins peut conduire vers un tout autre site web). Pour éviter des renvois frauduleux, une option est de privilégier la saisie des URL directement dans la barre d'adresses.*

Exemple d'un mail de « spear phishing » :


From [redacted]@outlook.com>
To [redacted]
Subject: Hungary's written comments

Dear Colleagues,

Proposal for a regulation of the European Parliament and the Council on the management of situations related to the instruments used in the field of migration (Document no.: ST 15152/2021) Hungary's written comments.

attachment link: https://1drv.ms/[redacted]

Please see the attachment!

Best regards,

Ms [redacted]
JHA Counsellor for migration and asylum
belügyi szakdiplomata – migráció és menekültügy

Permanent Representation of Hungary to the EU/ Magyarország Európai Unió melletti Állandó Képviselete
B-1040 Brussels, Rue de Trèves 92-98.
Tel.: + [redacted], Fax.: + [redacted]
GSM: + [redacted]
E-mail: [redacted]@mfa.gov.hu

Illustration - site Internet original :

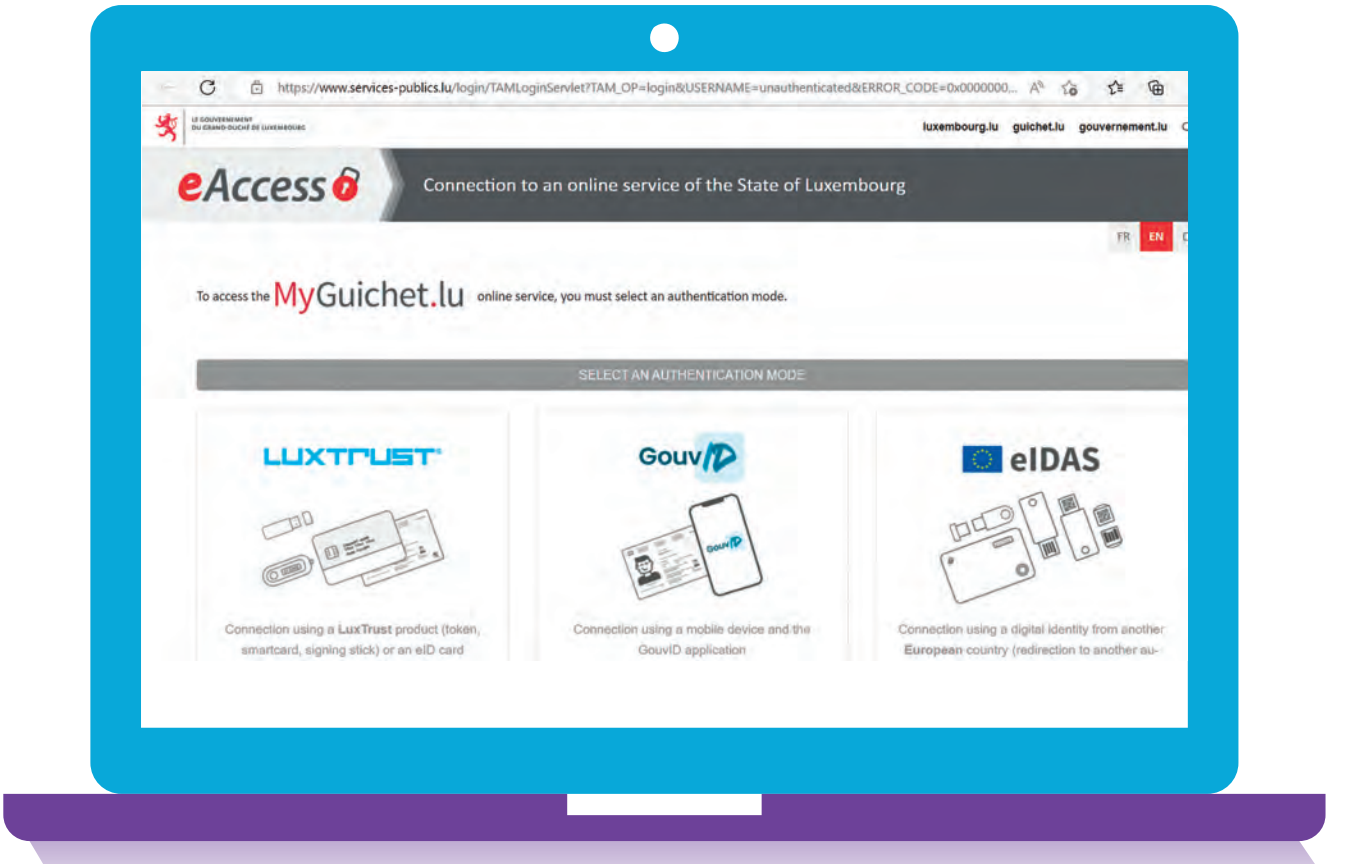


Illustration - site Internet corrompu :

L' « ingénierie sociale » (« social engineering »)

L'ingénierie sociale est une technique de manipulation humaine qui consiste à obtenir de la victime un bien ou une information à laquelle celle-ci peut accéder, directement ou indirectement, en exploitant sa confiance, son ignorance ou sa naïveté. Le facteur humain est le point central de ce type d'attaque.

L'attaque d'ingénierie sociale peut survenir dans la vie de tous les jours ainsi que sur le lieu de travail. Pour extorquer des informations ou des biens, il n'est pas rare que l'attaquant étudie au préalable les environnements personnel et professionnel de sa future victime afin d'établir, dans une première phase, une relation de confiance avec cette dernière.

Souvent les attaquants se dotent d'une connaissance approfondie du jargon employé par l'administration et des procédures mises en place par celle-ci. Cette manière de procéder facilite la prise de contact et permet de rendre la demande de l'attaquant crédible.

Les rapports entre l'attaquant et la victime peuvent prendre différentes formes. Elles peuvent notamment se faire via :

TÉLÉPHONE | **RÉSEAUX SOCIAUX** | **MAIL** | **PRÉSENCE PHYSIQUE DE L'ATTAQUANT**

Les moyens de prévention :

- *prendre le temps de réfléchir et éviter les décisions impulsives sous la pression de l'attaquant (ex. : ne pas divulguer ses identifiants ni son mot de passe, même si la demande semble crédible) ;*
- *ne pas révéler d'informations confidentielles sur les réseaux sociaux ;*
- *ne pas répondre à des demandes d'informations, voire à des instructions illicites ou émanant de sources non vérifiées ;*
- *rester vigilant dès qu'une personne inconnue adopte un comportement trop curieux, en particulier en ce qui concerne les activités professionnelles de l'agent.*

La « fraude au président »

La fraude au président consiste en l'usurpation de l'identité d'un membre de la direction de l'administration.

L'objectif de cette attaque est de convaincre l'agent que la demande ou l'ordre émane de sa hiérarchie et de l'inciter ainsi à effectuer une démarche bénéfique à l'attaquant, telle qu'un transfert d'argent sur un compte bancaire.

La plupart du temps, une fraude au président se déroule en **3 étapes** :

1. L'attaquant analyse l'environnement de l'administration et collecte toutes sortes d'informations disponibles (ex. : annuaire, organigramme, rapports annuels).
2. L'attaquant se fait passer auprès de l'agent pour un membre de sa hiérarchie dont il a usurpé l'identité.
3. L'attaquant utilise l'identité usurpée pour inciter l'agent à effectuer une démarche à son bénéfice, que ce soit par des moyens élaborés (ex. : mail contrefait en combinaison avec des techniques d'ingénierie sociale) ou non (ex. : appel téléphonique avec un numéro masqué).

Cela étant dit, il existe également d'autres formes de ce type d'attaque par usurpation d'identité dans lesquelles l'auteur malveillant se fait passer pour un agent de l'administration (et non pas pour un membre de la direction), par exemple, pour demander au service des ressources humaines un changement de compte bancaire pour le virement de sa rémunération.

L'essor des nouvelles technologies, en particulier les avancées liées à l'intelligence artificielle, permet aux personnes malveillantes de disposer d'outils numériques accroissant la crédibilité de leur attaque. Parmi ces techniques figure notamment celle de la « Deepfake voice » consistant en la création d'une voix de synthèse imitant la voix d'une personne à partir d'enregistrements sonores et vidéos collectés par l'attaquant.

Les moyens de prévention :

- *respecter les procédures de vérifications et de signatures multiples, en particulier pour les transactions bancaires ;*
- *porter un regard critique sur les demandes ou instructions inhabituelles ;*
- *accentuer la vigilance lors des périodes de congés scolaires, jours fériés ainsi que de manière générale en dehors des heures de bureau ;*
- *contacter immédiatement la hiérarchie avec les coordonnées officielles (ex. : annuaire de l'Etat) en cas de doute et s'abstenir d'exécuter définitivement les démarches sollicitées sans confirmation complémentaire ;*
- *ne pas céder à la pression de l'attaquant.*

Le « rançongiciel » (« ransomware »)

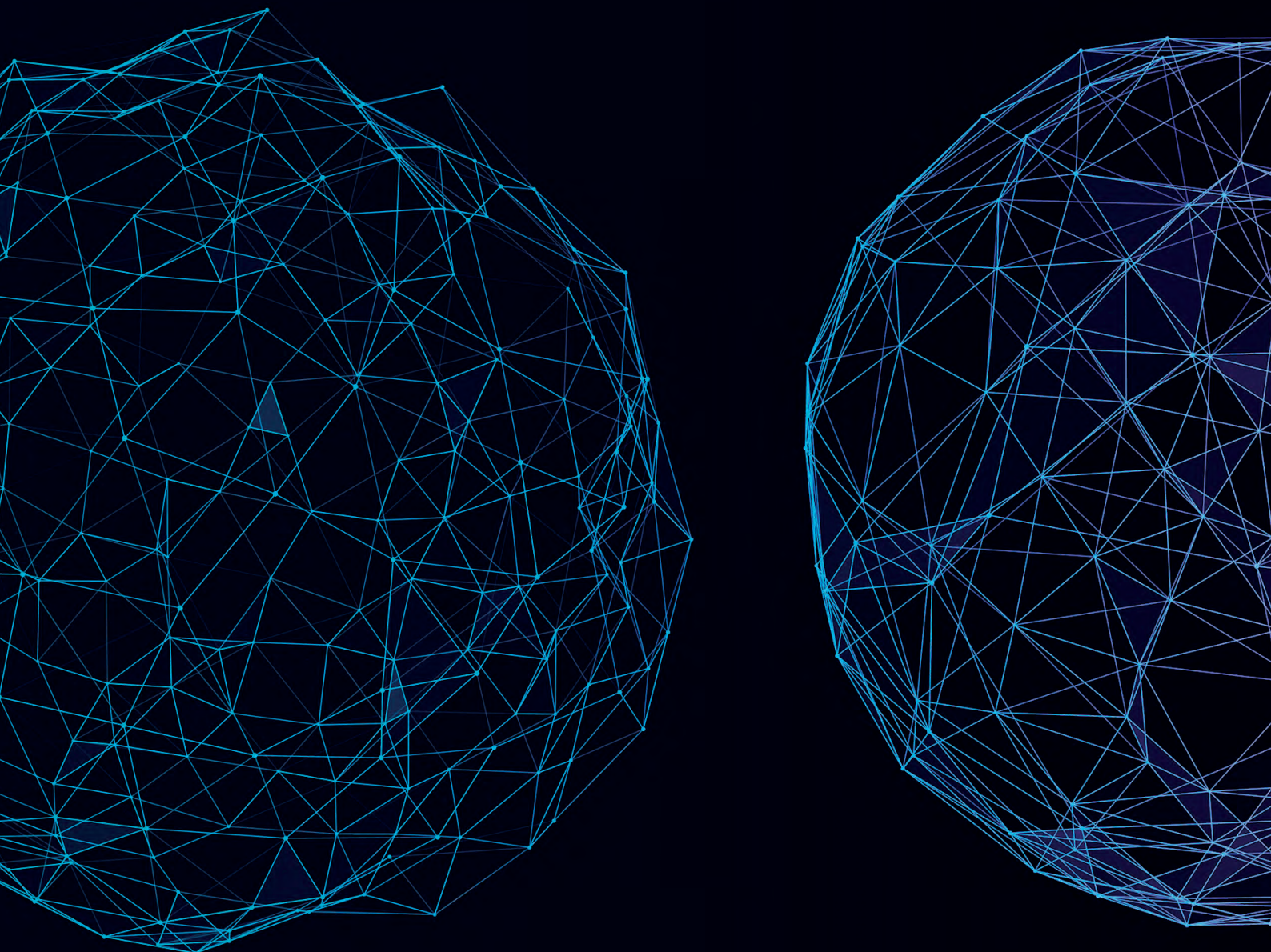
Le ransomware est un type de cyberattaque qui consiste en l'introduction d'un programme malveillant dans les systèmes informatiques de la victime qui chiffre les informations y contenues. La plupart du temps, le ransomware est lancé par une action de l'utilisateur et plus rarement par une vulnérabilité technique permettant son entrée dans le réseau interne.

Le but de cette attaque est de rendre impossible la consultation et l'utilisation des informations par la victime. Ceci permet à l'attaquant d'extorquer à cette dernière le paiement d'une rançon en contrepartie de la clé de déchiffrement, voire de la garantie qu'il ne va pas vendre ou publier les informations en question.

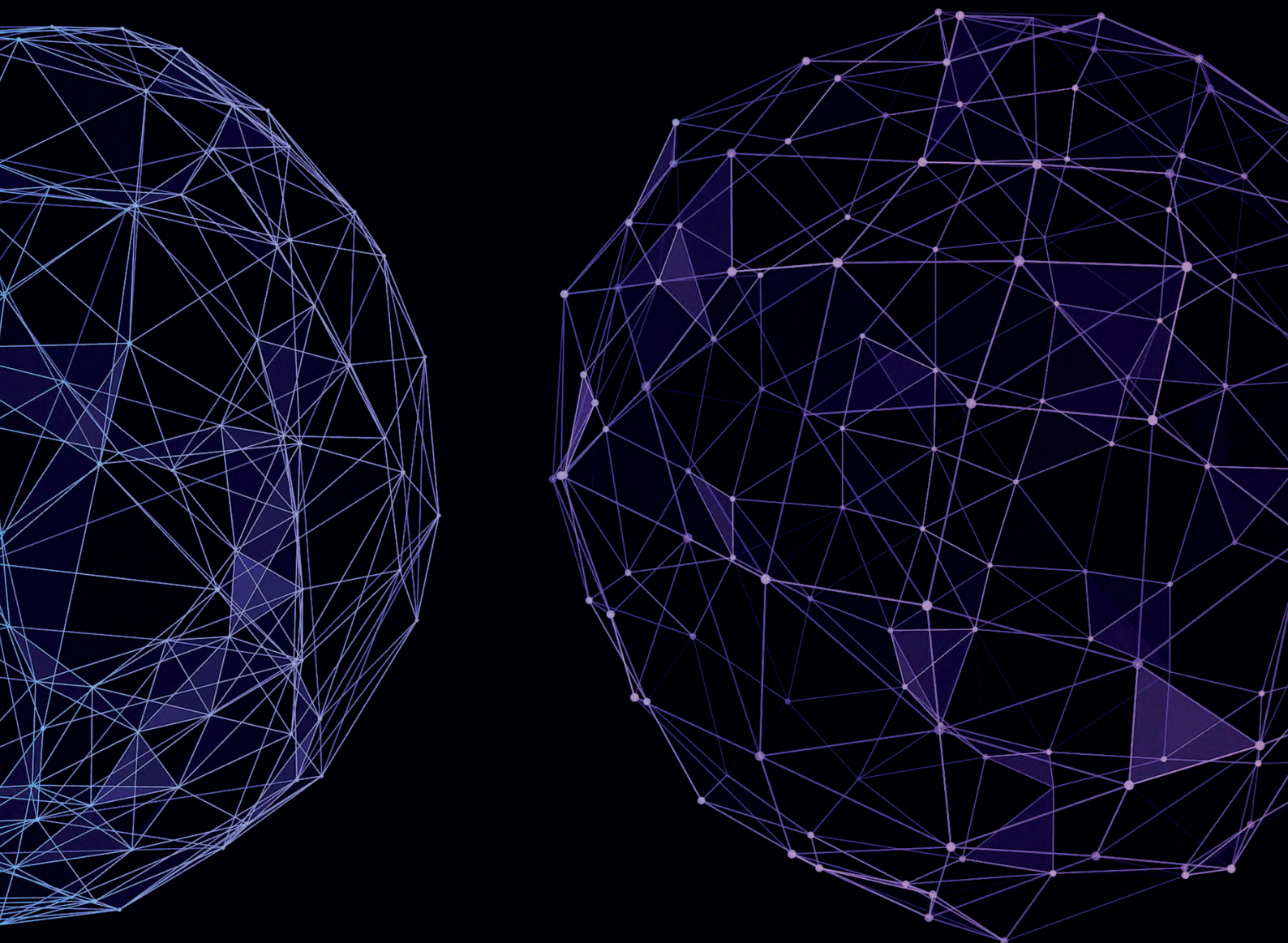
A noter que l'Agence de l'Union européenne pour la cybersécurité (« ENISA ») a rapporté une augmentation de **234 %** *du nombre d'attaques par ransomware en 2021. En raison de cette évolution significative, l'ANSSI a élaboré des recommandations en la matière.*

Les moyens de prévention :

- *rester prudent lors de l'ouverture de mails, pièces-jointes ou liens suspects ;*
- *mettre à jour régulièrement les systèmes informatiques et applications ;*
- *ne pas installer de logiciels sans l'autorisation de l'administration ;*
- *en cas de suspicion de corruption de systèmes ou fichiers, contacter sans délai l'instance gestionnaire des incidents de sécurité interne désignée par l'administration et, en particulier, le GOVCERT ;*
- *en cas de suspicion de corruption de systèmes ou fichiers, débrancher la machine touchée par l'attaque du réseau d'Internet en vue d'éviter la propagation du programme malveillant dans les systèmes informatiques de l'administration ;*
- *ne pas éteindre la machine infectée (sans préjudice de l'obligation de débrancher la machine d'Internet) afin d'éviter toute perte de preuves et de traces liées à l'incident de sécurité.*



COMMENT RÉAGIR EN CAS DE SOUPÇON D'UN INCIDENT DE SÉCURITÉ OU D'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL ? //



LE RÔLE CENTRAL DE L'AGENT DANS LA DÉTECTION ET LA REMONTÉE DES INCIDENTS DE SÉCURITÉ

L'agent a un rôle important à jouer afin de permettre à son administration de détecter les incidents de sécurité et les violations de données et de les gérer de manière appropriée.

L'agent doit :

- **informer, sans délai, l'instance gestionnaire des incidents de sécurité de l'information désignée par l'administration de tout soupçon d'incident de sécurité**, qu'il s'agisse ou non d'une violation de données ;
- **rapporter les faits qu'il a observés ainsi que les actions qu'il a entreprises**, en particulier juste avant et au cours de l'incident de sécurité, avec le plus de précision possible.

L'objectif de cette documentation et de cette remontée d'informations par l'agent est de permettre à l'administration de parvenir à une compréhension détaillée de l'incident.

LES BONNES PRATIQUES À RESPECTER PAR L'AGENT EN CAS DE SOUPÇON D'UN INCIDENT DE SÉCURITÉ

L'agent doit mettre en œuvre les bonnes pratiques en cas de soupçon d'un incident de sécurité. Ainsi, il doit notamment :

1

Remonter des informations dans les meilleurs délais au niveau approprié

Le premier réflexe de l'agent doit être de contacter l'instance gestionnaire des incidents de sécurité de l'information désignée par son administration, dès qu'il a des raisons de soupçonner qu'un incident de sécurité (qu'il s'agisse ou non d'une violation de données) se produit ou est susceptible de se produire.

En pratique, il s'agit le plus souvent du :

- *supérieur hiérarchique,*
- *support informatique de l'administration,*
- *RSSI, si désigné par l'administration, CTIE et GOVCERT,*
- *DPD.*

La réactivité de l'agent est essentielle. En effet, plus vite un incident sera signalé, plus les chances sont grandes d'en limiter les conséquences néfastes pour l'administration et pour les personnes concernées.

Ne pas dissimuler ou minimiser l'incident

L'agent doit signaler tout incident de sécurité potentiel avec le maximum de détails possible. Il ne doit pas omettre de faits liés à l'incident de sécurité ou en diminuer leur gravité, notamment en raison d'un sentiment de honte lié à son erreur, par crainte des conséquences éventuelles de ses actes (souvent l'agent étant lui-même victime), voire pour réduire son implication potentielle dans la production de l'incident (ex. : mauvaise manipulation).

2

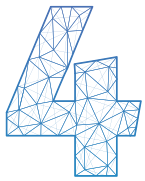
Ne pas effectuer de qualification juridique de l'incident de sécurité

A moins que ce rôle ait expressément été attribué à l'agent par sa hiérarchie, il n'est pas de sa compétence de faire une analyse juridique et technique de la situation, voire une qualification juridique des faits (ex. : s'agit-il ou non d'une violation de données à caractère personnel au sens du RGPD ?).

Le rôle de l'agent consiste principalement à remonter des informations nécessaires au niveau approprié afin d'informer les services compétents de la survenance d'un incident potentiel. Il revient ensuite à ces services (ex. : le DPD, le RSSI, le CTIE, le GOVCERT) d'évaluer les démarches à entreprendre et de déterminer si un incident de sécurité de l'information est à qualifier de violation de données au sens du RGPD.

Ne pas essayer de résoudre seul le problème

En cas de soupçon d'un incident de sécurité, **l'agent doit s'abstenir de toute tentative de résoudre le problème de sa propre initiative**. Il doit agir sur base des procédures internes en vigueur ou sur base des instructions communiquées par l'instance gestionnaire des incidents de sécurité de l'information et informer les personnes en charge des violations de données.



5

Ne pas divulguer des informations confidentielles

L'obligation de confidentialité de l'agent ne s'éteint pas avec la survenance potentielle d'un incident de sécurité.

De ce fait, **l'agent doit rester vigilant et ne pas divulguer des informations relatives à l'incident à des personnes non autorisées**, tant pendant qu'après la survenance de l'incident.

Déconnecter la connexion Internet en cas de soupçon d'une cyberattaque

En cas d'un soupçon d'une cyberattaque, **l'agent doit immédiatement déconnecter sa machine du réseau Internet**, avec fil (par câble « Ethernet ») ou sans fil (ex. : Wifi, Bluetooth). Il doit également déconnecter toutes les machines qui seraient reliées à la sienne ou branchées sur le même réseau.

Le fait de déconnecter la machine évite la propagation de malwares, tels que les virus, dans les systèmes informatiques de l'administration.

6

Si l'agent constate un dysfonctionnement de sa machine (ex. : lenteur de réaction, ouverture de fichiers erronés, cryptage des informations en direct), il est possible, voire probable, qu'une attaque du type ransomware soit en train de se produire.

Dans pareil cas de figure, l'agent doit immédiatement déconnecter toutes les machines de son poste de travail susceptibles d'être infectées afin de confiner le malware. Par contre, comme évoqué ci-dessous, il ne doit jamais les éteindre pour éviter toute perte de preuves et de traces.

7

Ne pas débrancher la machine du réseau d'électricité, ni l'éteindre en cas de soupçon d'une cyberattaque

L'agent ne doit **pas retirer la prise électrique de sa machine, ni l'éteindre** en cas de soupçon d'une cyberattaque (sans préjudice de l'obligation de déconnecter la machine d'Internet) afin d'éviter toute perte de preuves liées à l'incident de sécurité.

Une partie des preuves liées aux attaques malveillantes sont sauvegardées sur la « mémoire vive » (la « RAM ») de chaque machine, c'est-à-dire sur la mémoire à court terme de la machine, où sont stockées les données actuellement utilisées par le processeur.

Compte tenu du fait que cette mémoire vive est effacée à chaque fois que la machine est éteinte ou redémarrée, l'agent doit s'abstenir d'entreprendre une telle démarche et veiller à ce que la machine ne s'éteigne pas ou ne redémarre pas à cause d'un acte externe (ex. : perte de batterie ou coupure d'électricité).

Sécuriser les preuves

Afin de faciliter le travail des experts en « data forensics », l'agent doit **documenter les faits, les actions entreprises ou observées ainsi que les évènements liés à l'incident de sécurité.**

La « data forensics » est une branche des sciences criminalistiques qui porte sur la recherche, l'acquisition, le traitement et l'analyse de données stockées sous forme numérique et sur la communication d'informations les concernant.

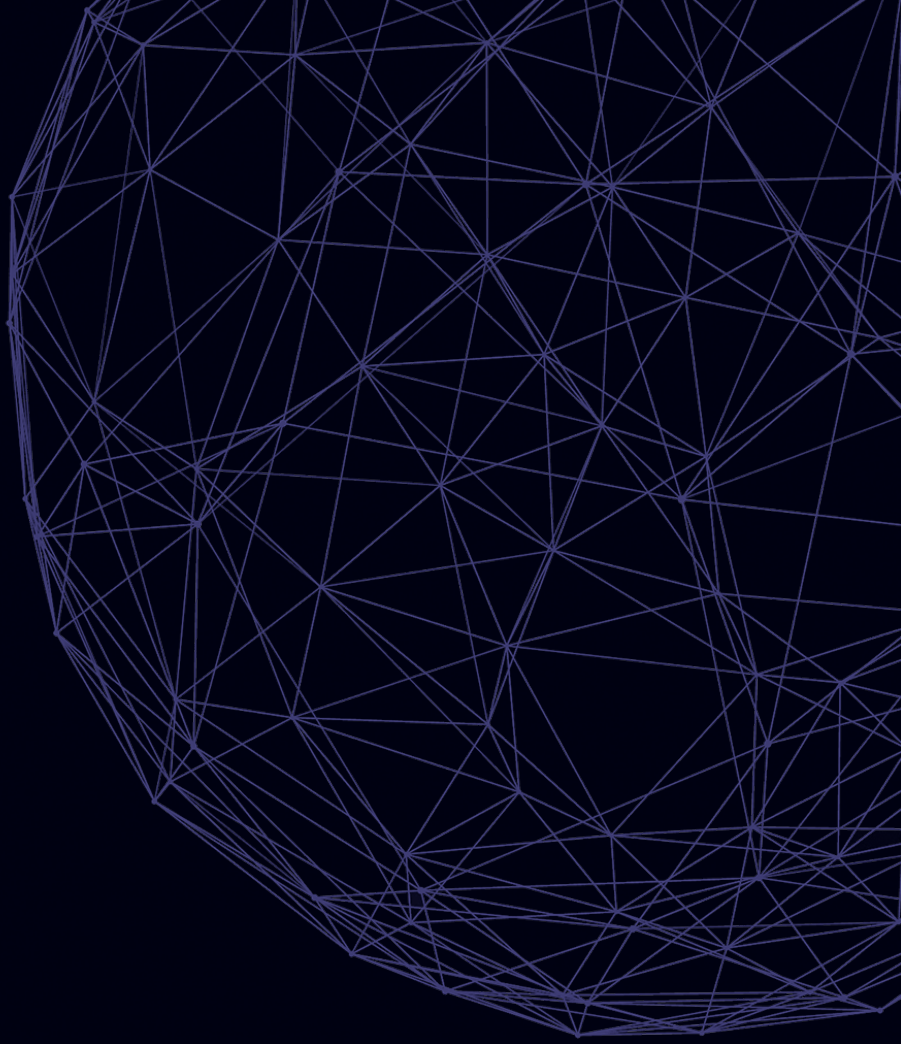
La documentation doit *a minima* comprendre :

- l'identité des personnes impliquées dans le déroulement et la gestion de l'incident de sécurité ;
- une description chronologique détaillée de chaque action entreprise ou observée ainsi que des faits et évènements constatés (avec les dates et heures).

Dans une optique de documentation de l'incident de sécurité, des vidéos ou des photos de toute activité suspecte peuvent être prises par l'agent. Cette démarche sera utile aux experts en la matière pour contextualiser et comprendre l'incident de sécurité.

Changer le mot de passe en cas de compromission (réelle ou suspectée)

Dans l'hypothèse où une **compromission du mot de passe** est suspectée, **l'agent doit le modifier** dans les plus brefs délais afin de prévenir toute utilisation illicite par des tiers (sans préjudice de l'obligation de désactiver le compte en cas de doute).



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État

En collaboration avec :

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Haut-Commissariat
à la protection nationale

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

CERT gouvernemental

ctie
Centre des technologies
de l'information de l'État

LHC
Luxembourg House
of Cybersecurity

CNPD
COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

ILR
INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

CCSS
Centre commun de
la sécurité sociale