MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Gendarmerie nationale

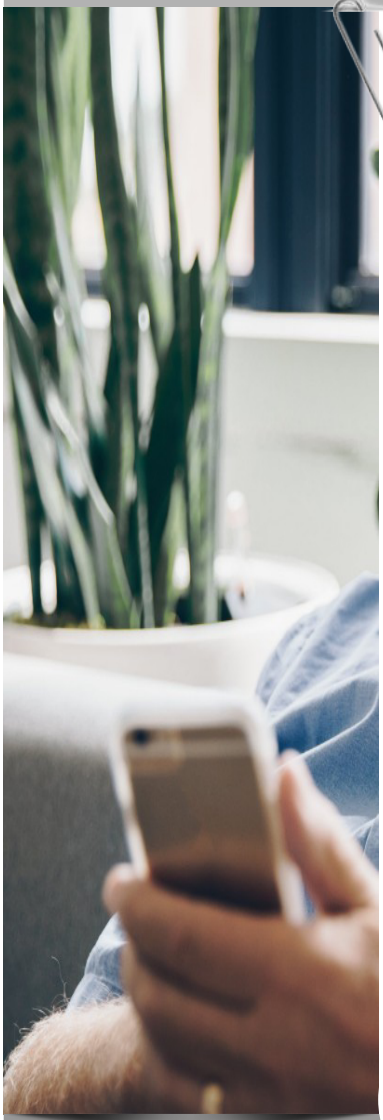
Petit Logiciel Illustré

Entreprise & Cybersécurité

ComCyberGend

Réserve citoyenne
Engagée à vos côtés

Réalisons un questionnaire test



1. Avez-vous établi une **cartographie** précise et actualisée de votre système informatique ? *(En clair, pouvez-vous dire quels sont vos supports numériques, où ils sont connectés, qui s'y connecte et quand ?)*

2. Avez-vous établi une **charte de sécurité**, à laquelle vos collaborateurs et vous-même avez adhéré ?

3. La gestion du système d'information est-elle limitée à un niveau **Administrateur** ?

4. Les **mots de passe** sont-ils individuels et suffisamment robustes ?

5. Avez-vous établi des procédures pour les **mises à jour** ?

6. Avez-vous un protocole standardisé pour vos **sauvegardes** ?

7. Avez-vous une solution de **sécurité** adaptée à votre ordinateur et à chaque périphérique ?

8. Y a-t-il une politique de sécurité liée à la gestion des périphériques **USB** dans votre entreprise ?

9. Lors de vos déplacements ou ceux de vos collaborateurs sécurisez-vous votre connexion **(VPN)** ?

10. Avez-vous formé votre équipe aux mesures de prudence lors de l'utilisation de leur **messagerie**, et des traces qu'ils laissent sur internet *(identité 3.0)* ?

- ***Vous avez obtenu moins de 10 affirmations ?***
- ***Alors ce guide peut vous aider***

Sommaire

édito

En matière de sécurité numérique, les risques sont présents à l'intérieur de votre entreprise comme à l'extérieur. Nous envisagerons donc ces deux situations.

Vous trouverez dans ce guide, des questions, suivies d'explications qui vous permettront de répondre. ”

Les risques et les conséquences

“Les cyber-attaques coûtent cher, très cher aux entreprises, non seulement financièrement mais aussi humainement, et peuvent mettre en jeu votre réputation.”

Les risques encourus...

√ **la perte de données de travail sur les clients ou la comptabilité**

√ **la perte de marchés et la dégradation de l'image par le vol de fichier, la divulgation d'informations confidentielles, le vol ou le détournement de site WEB.**

√ **la perte financière**

√ **la perte de temps**

√ **le problème environnemental** *(attaques bactériologique, chimique et nucléaire...)*

...en connaître les conséquences

√ **l'impact sur la conception, la production et la distribution**

√ **la perte de confiance, de crédibilité**

√ **la remise en cause de l'éthique et le coup de frein à l'innovation**

√ **la perte de chiffre d'affaires, la perte de confiance des actionnaires et les pénalités de retard**

√ **l'arrêt de la production, la recherche des causes et la remise en état du système**

√ **le risque vital**

souvenez-vous !

L'origine des attaques

“ Les attaques sont en majorité d'origine humaine...

- ⇲ **"keylogger"** *(enregistreur de frappe)*
- ⇲ **virus, malwares**
- ⇲ **hameçonnage**
- ⇲ **lien vidéo**
- ⇲ **nom de domaine imitant le nom officiel** *(en cliquant sur une pièce jointe)*
- ⇲ **insertion de virus dès la programmation**

...mais peuvent venir d'une faille de sécurité dans la programmation du microprocesseur ! ”

souvenez-vous !

Les objectifs sont multiples.

Il peut s'agir de jeu ou de malveillance.

Le but des attaques

- *Espionnage*
  Renseignement
  Intelligence économique
- *Extorsion d'argent*
- *Malveillance*
  Vengeance
- *Neutralisation*
  Sabotage
  Destruction
- *Pré-positionnement stratégique (invasion)*
- *Idéologie*
  Agitation
  Propagande
- *Jeu*
  Exploit

À l'intérieur de l'entreprise

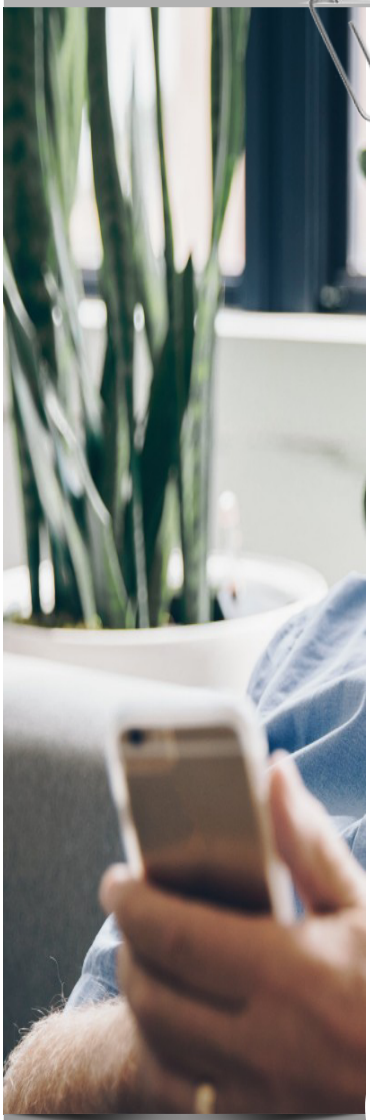
- **Vous trouverez pour chaque chapitre :**
- **des questions pour évaluer votre entreprise,**
- **des explications,**
- **des solutions.**

A – LES ORDINATEURS, TABLETTES, TÉLÉPHONES.
1. Les ordinateurs : compte Administrateur
2. Les mots de passe
3. Les logiciels : mise à jour
4. Sauvegarde et stockage des données

B – LES PÉRIPHÉRIQUES
1. Les risques
2. Les contre-mesures logicielles
3. Les contre-mesures matérielles
4. Les contre-mesures comportementales

C – LE WEB : INTERNET & INTRANET
1. Connexion Internet
2. La messagerie *(mails)*
3. Recherche Internet *(surf)*
4. Site web

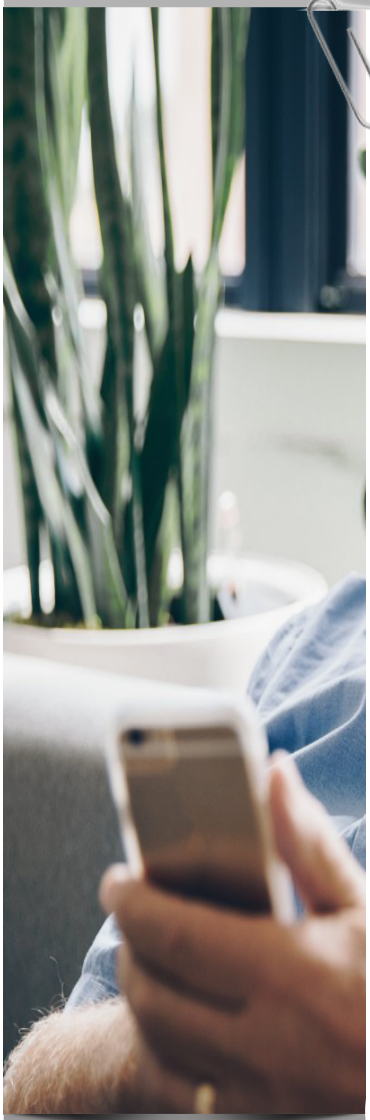
Réalisons un questionnaire test



1. Disposez-vous d'un antivirus ?
2. Disposez-vous d'un pare-feu *(firewall)* ?
3. Avez-vous des outils de filtrage et de journalisation de l'activité ?
4. Utilisez-vous un logiciel de chiffrage codé ?
5. Si vos données sont particulièrement sensibles ou confidentielles, votre système est-il isolé en Air Gap ? ①
6. Effectuez-vous régulièrement des mises à jour de votre ordinateur ?
7. Votre antivirus est-il régulièrement mis à jour suivant un protocole ?
8. Existe-t-il un poste dédié à Internet, séparé des postes accédant à l'intranet ?
9. Les salariés sont-ils sensibilisés à l'utilisation à titre personnel du matériel professionnel ?
10. Les salariés travaillent-ils à leur domicile via une connexion ?
11. Procédez-vous à des sauvegardes quotidiennes, dont l'une hors ligne ?
12. Le recyclage ou la destruction de vos ordinateurs et de vos supports de sauvegarde devenus obsolètes font-ils l'objet d'un protocole particulier ?
13. Avez-vous conscience que vos tablettes et vos smartphones sont des ordinateurs, et qu'ils en ont la même vulnérabilité ?
14. L'installation téléphonique est-elle sécurisée ?

① *Un air gap, ou air wall, est un dispositif d'isolement physique d'un système de tout réseau informatique. Ce dispositif rend toute tentative de piratage à distance impossible.*

Réalisons un questionnaire test



1. Avez-vous une cartographie précise et actualisée du réseau informatique ?

2. Les écrans sont-ils conçus, orientés, ou équipés afin que seul l'utilisateur installé bien en face puisse voir l'affichage ?

3. Votre système informatique est-il configuré en réseau ?

4. Êtes-vous vigilant quant aux opérations de télémaintenance informatique ?

5. Avez-vous un compte administrateur restreint ?

6. L'administrateur réseau est-il extérieur à l'entreprise ?

7. L'administrateur réseau peut-il intervenir de manière autonome ?

8. Les mots de passe comportent-ils au moins dix caractères mélangeant lettres majuscules, lettres minuscules, chiffres et symboles ?

9. Les mots de passe sont-ils changés régulièrement ?

10. Les mots de passe sont-ils individuels ?

11. Les ordinateurs se mettent-ils en veille après une minute d'inutilisation, avec réactivation par introduction du mot de passe ?

12. Éteignez vous les ordinateurs lorsqu'ils ne sont pas utilisés durant une longue période ?

13. Utilisez-vous des bouchons USB pour recharger vos équipements sur des ports USB prévus à cet effet ?

Par ailleurs

1. Les prestataires extérieurs habituels *(ménage, maintenance informatique…)* font-ils l'objet d'une attention particulière et régulière ?

2. Les stagiaires et intérimaires sont-ils effectivement encadrés et sensibilisés à la confidentialité ? *(accompagnement en permanence dans les déplacements à l'intérieur de l'entreprise)*

3. Avez-vous une politique de contrôle des rapports de stage ?

4. Tenez-vous un registre des visiteurs ?

5. Les visiteurs ont-ils tous des badges avec accès restreint ?

6. Faites-vous déposer les téléphones et matériels de prise de vue à l'accueil ?

7. La mise à disposition de matériel informatique au personnel extérieur est-il sécurisé ? *(ordinateur dédié, réseau spécifique, code d'accès spécifique, accès réseau restreint…)*

8. L'utilisation des photocopieurs et scanners par des personnes extérieures à l'entreprise est-elle encadrée ?

9. Avez-vous prévu un système informatique sécurisé, non accessible aux personnes étrangères à l'entreprise ?

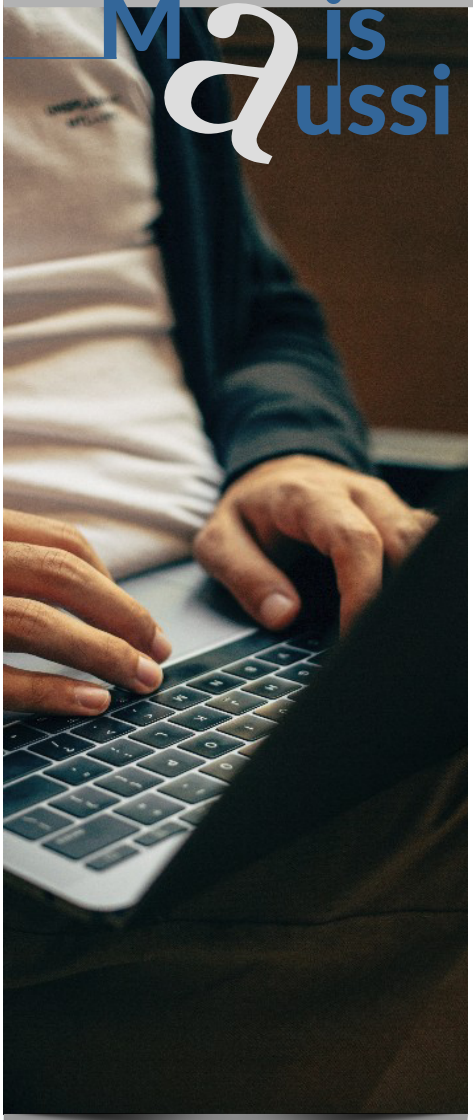
10. Lorsqu'une clé USB ou un disque dur externe sont perdus ou volés, pouvez-vous les désactiver, ou reconfigurer le mot de passe à distance ?

11. Avez-vous une politique de recyclage de vos disques durs internes ?

12. Avez-vous gardé une sauvegarde lors de chaque mesure de prévention *(chiffrement, changement de mot de passe etc.)* ?

Réalisons un questionnaire test

Mais aussi



1. Avez-vous désigné au sein de votre entreprise, un responsable de la sécurité informatique ?

2. Avez-vous élaboré une charte de sécurité informatique ?

3. Avez-vous formé l'ensemble de vos salariés à ces consignes de sécurité *(comportement, savoir-faire, conduite de crise)* ?

4. Sensibilisez-vous régulièrement votre personnel à ces consignes d'hygiène informatique ?

5. Contrôlez-vous régulièrement l'application de ces mesures ?

6. Sensibilisez-vous les cadres occupant un poste stratégique ?

7. Incluez-vous des clauses de confidentialité dans les contrats de travail *(stagiaires, prestataires extérieurs)* ?

Les ordinateurs, tablettes, téléphones

1. Les ordinateurs explications & solutions

> ***Un ordinateur est une boîte qui possède plusieurs pièces physiques qui ont chacune leur importance.***

Il faut inclure également les tablettes, smartphones, imprimantes, la robotique, la domotique, les appareils électroménagers, les machines-outils, qui sont des mini-ordinateurs.

Il fonctionne
d'une part grâce au système d'exploitation, d'autre part avec des logiciels spécifiques.

• ***Le système d'exploitation, logiciel système :*** c'est l'ensemble des programmes qui pilotent les différents composants de l'appareil informatique. C'est l'interface entre l'utilisateur et le matériel informatique.
• Il permet de faire fonctionner les différents périphériques *(souris, clavier…)*
Sans lui l'ordinateur ne fonctionne pas *(Android, iOS, Mac Os, Linux, Windows…)*.
• Il permet l'exploitation des données et se retrouve au niveau des programmes informatiques, des jeux, des réseaux *(Internet, extranet, jeux)*.

Les logiciels applications : ils sont dédiés à des tâches spécifiques
• ils relient les ordinateurs de l'entreprise entre eux *(via un serveur intranet)*
et /ou
• ils relient certains ou tous les ordinateurs au réseau mondial d'Internet *(extranet)* avec tous ses services, ses vulnérabilités et sa sécurité.

Il est donc important de connaître la cartographie précise des ordinateurs et des connexions ; cela permet d'identifier rapidement l'origine des attaques.

Par ailleurs, il faut orienter l'écran de telle sorte que seul l'utilisateur puisse le voir.

Les ordinateurs, tablettes, téléphones

1. Le compte Administrateur

« Au démarrage, la session Administrateur apparaît : c'est la session qui gère tous les ordinateurs. Pour travailler utilisez une session Utilisateur. »

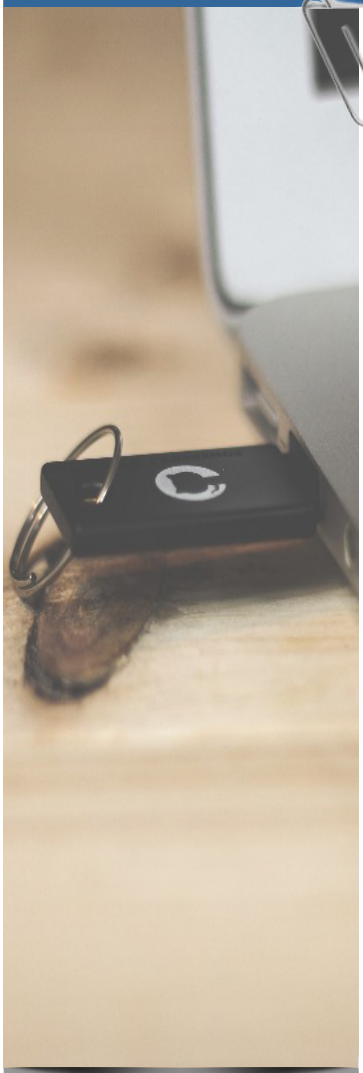
RETENEZ BIEN CECI !

1. Le compte Administrateur est utilisé pour intervenir sur le fonctionnement global de l'entreprise notamment la mise à jour de logiciels. Pour votre utilisation quotidienne, utilisez un compte Utilisateur.

2. Établissez une cartographie précise et actualisée du réseau informatique de votre entreprise, c'est-à-dire identifiez précisément les utilisateurs du système, nommément, et les privilèges qui leur sont accordés *(tous n'ont pas accès au compte Administrateur)* ; l'identification permet de relier, à un Utilisateur, une action sur le système.

3. Encadrez par des procédures codifiées les arrivées et les départs de personnels pour que leurs droits sur les systèmes d'information soient au plus juste et qu'à leur départ ils leur soient supprimés.

4. Nommez un responsable informatique pour veiller à toutes les procédures.



Sécurisez vos ordinateurs

> *Pour que chaque session soit protégée voici nos préconisations »*

1. Mot de passe sécurisé par session : il ferme à clé votre maison.

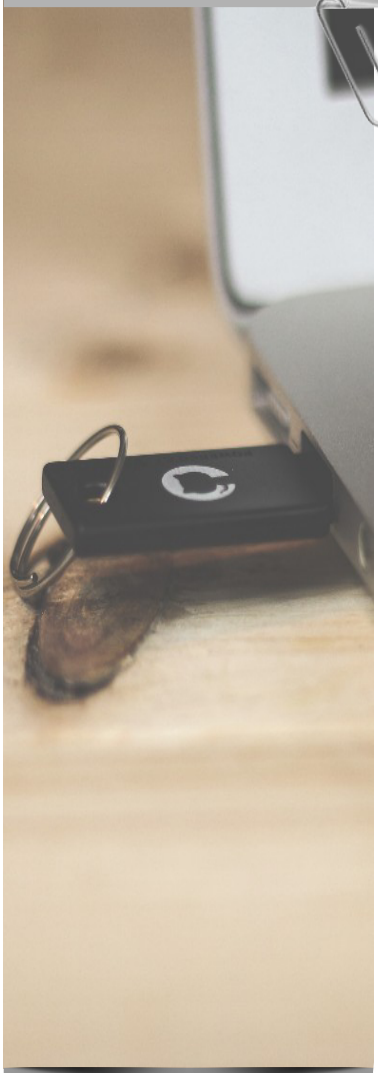
2. Session Administrateur non reliée à Internet ; utilisez plutôt un autre objet connecté. Si vous laissez la clé sur la porte, quelqu'un qui entrerait de l'intérieur *(via Internet)*, pourrait avoir accès à vos données *(les connections sortent sur Internet, mais peuvent également entrer)*.

3. Des sessions séparées, différentes : la clé de la porte principale *(porte d'entrée ou jardin)*, c'est le mot de passe de la session Administrateur. Vous, le gérant de la société, et/ou le responsable informatique, êtes le seul détenteur, et le garant de la sécurité de l'entreprise.

4. Mots de passe des autres sessions : chaque collaborateur a le sien, c'est la clé de son bureau.

5. Extinction des ordinateurs lors des absences : longues ou mise en veille avec verrouillage *(il y aura nécessité de réactiver par le mot de passe après une minute d'inutilisation)* de la même façon que vous fermez votre porte lors de vos déplacements.

6. Écrans correctement orientés ou équipés de filtres afin que seul l'utilisateur installé bien en face puisse voir l'affichage *(vous mettez bien des rideaux aux fenêtres, pour protéger votre intimité)*.



2. Le mot de passe

« Le mot de passe est extrêmement important : c'est la clé qui permet d'entrer dans votre ordinateur. »

Il doit impérativement être composé de la manière suivante :

↪ 12 caractères

↪ majuscule, minuscule, chiffre, caractères spéciaux

↪ aucun lien avec vous, ni votre famille *(pas de date de naissance, prénom, nom…)*

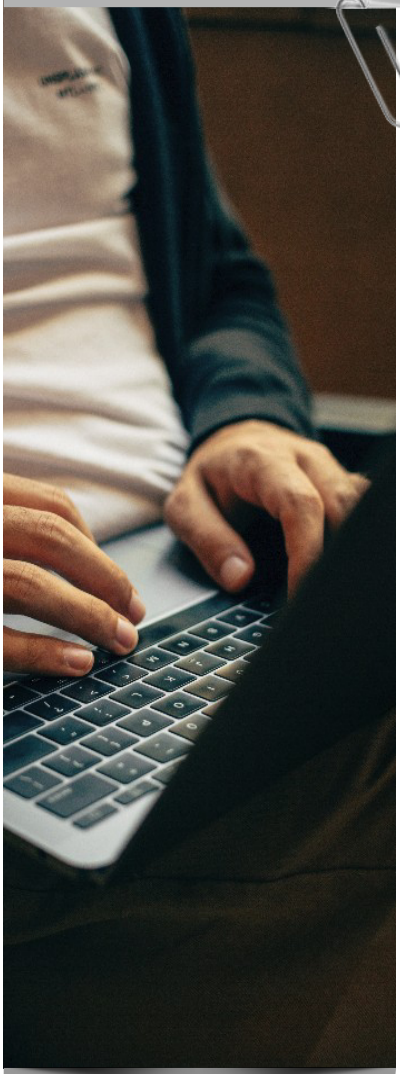
↪ un mot de passe différent par objet et par service sensible

↪ ***ne pas stocker les mots de passe :*** pas de post-it™, papier, outil de stockage numérique (*sauf logiciel gestionnaire de mots de passe avalisé)*

↪ changer les mots de passe initiaux établis par défaut *(imprimante, box, serveur…)*

↪ les changer régulièrement tous les six mois

Exemple :
↪ première lettre d'une phrase : je change mon mot de passe tous les six mois
=JcMmDptl6m!
↪ ou phonétique : j'ai un mot de passe sécurisé en 12 caractères
G1mOdpcCu12/



3. Les logiciels de l'ordinateur

La mise à jour

> ***Dans chaque système d'exploitation, chaque logiciel, chaque application, il existe des failles, des zones de vulnérabilité pouvant être attaquées pour fragiliser, utiliser ou anéantir les données.***

C'est pourquoi, quand ces failles sont découvertes, les éditeurs proposent des mises à jour aux utilisateurs.

RETENEZ BIEN CECI !

Soyez prudent dans les téléchargements :

1) ne pas télécharger si l'on demande un accès à vos données ;

2) ne pas télécharger de logiciel associé.

"Pour reprendre l'exemple de votre maison, dès que vous avez une fissure dans le mur, réparez-la, avant que votre mur ne s'écroule".

Sécurisez vos mises à jour

« Les logiciels contenus dans l'ordinateur doivent être mis à jour. Ces mises à jour sont extrêmement importantes, elles permettent de régénérer le programme du logiciel mais aussi d'incorporer les améliorations, notamment en matière de sécurité. »

	mise à jour classique	*mise à jour métier*
Effectuez-la régulièrement ou dès que l'éditeur demande une mise à jour	✓	✓
Établissez un protocole de mise à jour	✓	✓
Faites une sauvegarde sécurisée de vos données avant la mise à jour	✓	✓
N'utilisez que des sites officiels de l'éditeur	✓	✓
Configurez vos logiciels pour une mise à jour automatique	✓	
Dédiez une mise à jour particulière au poste Administrateur	✓	
Transférez sur le compte Administrateur, Internet éteint		✓
Utilisez l'antivirus pour faire une analyse		✓
Faites une copie sur disque dur externe		✓

4. Sauvegarde et stockage des données

“N’hésitez pas à prendre conseil ou faire rédiger les contrats par des spécialistes qui vous conseilleront de la manière la plus adaptée.”

La durée de vie des supports est également à prendre en compte.
Chiffrez vos données à l’aide d'un logiciel de chiffrement avant de les sauvegarder ; cela rendra impossible leur lecture.

Il faut impérativement prévoir des tests de sauvegarde *(un par semestre)* et les prévoir contractuellement avec le prestataire informatique.

Il est fondamental de sauvegarder et stocker ses données. Pour la plupart des entreprises et des États, les données vont devenir le nouvel « or noir ».

Pour simplifier, une sauvegarde peut s’effectuer sur différents supports, selon des techniques informatiques variées. Il s’agit des disques durs, CD, DVD, cartes mémoires, USB....

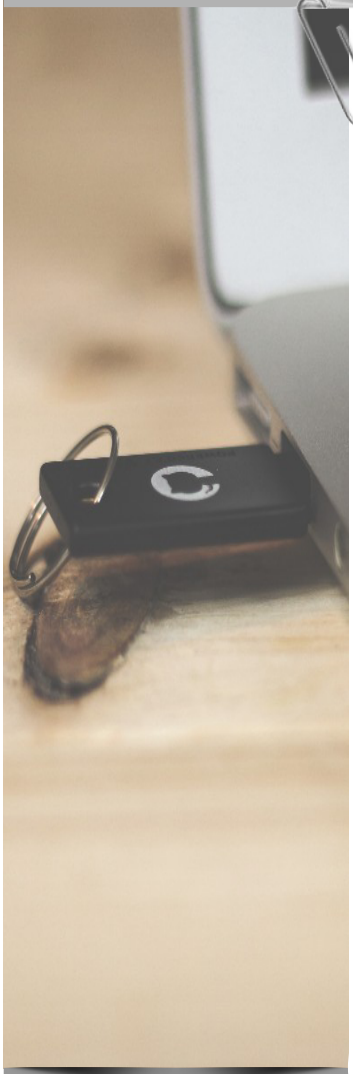
Les sauvegardes consistent à faire des copies régulières des fichiers à un instant T *(sur le même support ou un support différent)*, destinées à remplacer les fichiers originaux en cas de perte ou de corruption des données. Ces copies peuvent se faire manuellement ou automatiquement, la dernière solution évitant les oublis.

Questionnez-vous sur la durée de vie de votre support de sauvegarde.

Le stockage correspond à l’archivage des données. Il a l’avantage d’avoir une durée de vie de quelques années. De plus il permet de libérer de l’espace sur le disque dur.
La sauvegarde et le stockage sont l’assurance de votre maison.
Ils doivent être réguliers, si possible quotidiens.
Il est nécessaire de les faire sur au moins deux supports : disque dur externe, clé USB, cloud, deux sites distants.

- Pour le disque dur externe, le ranger à l’extérieur de l’entreprise pour éviter sa destruction en cas de dégât des eaux par exemple, ou de destruction par incendie.
- Pour le Cloud, vérifier les clauses du contrat : protection de la confidentialité, protection juridique en fonction du pays de stockage, garantie pour la disponibilité et l’intégrité des données et réversibilité du contrat.

Les ordinateurs, tablettes, téléphones



4. Sauvegarde et stockage des données

RETENEZ BIEN CECI !

- ↘ **Sauvegarder** quotidiennement vos données sur deux supports différents, dans des endroits différents
- ↘ **Vérifier** la durée de vie des supports
- ↘ **Tester** les sauvegardes chaque semestre
- ↘ **Vérifier** ou rédiger les clauses du contrat
- ↘ **Chiffrer** les données avant sauvegarde
- ↘ **Sauvegarder** particulièrement les données du poste Administrateur

4. Sauvegarde et stockage des données

RETENEZ BIEN CECI !

↘ Création d'une session Administrateur *(pour le gérant, ou le responsable informatique)*

↘ Création d'une session Utilisateur personnalisée pour chacun, y compris le gérant

↘ Nomination d'un responsable informatique

↘ Établissement d'une cartographie nominale du réseau informatique

↘ Encadrement des procédures d'arrivée et de départ *(fermer les sessions)*

↘ Choix d'un mot de passe sécurisé individuel pour chaque session et chaque activité

↘ Verrouillage automatique de la session

↘ Extinction en cas de longue absence

↘ Écrans protégés

↘ Formalisation des sauvegardes et du stockage des données

↘ Respect des procédures de destruction du matériel informatique

Réalisons un questionnaire test

1. Utilisez-vous des clés USB ou des disques durs externes dans votre entreprise ?
2. Les clés USB, les disques durs externes et les divers périphériques *(ou seulement l'un d'eux)* utilisés sont-ils exclusivement ceux fournis par l'entreprise ?
3. Parmi les périphériques fournis par l'entreprise, y en a-t-il qui soient publicitaires ou offerts ?
4. Utilisez-vous des périphériques de marque inconnue ou à bas prix ?
5. Sur les salons, en congrès, à l'hôtel, rechargez-vous vos téléphones mobiles ou vos ordinateurs sur des bornes USB ?
6. Faites-vous analyser les fichiers de vos périphériques par l'antivirus ?
8. L'exécution automatique des pilotes lors du premier branchement des périphériques est-elle désactivée ?
9. Lorsqu'ils ne sont plus utilisés, déconnectez-vous physiquement les périphériques, notamment les clés USB et les disques durs externes ?
10. Les périphériques utilisés, notamment les clés USB et les disques durs externes, sont-ils autorisés à sortir de l'entreprise ?
11. Avez-vous un protocole de recyclage ou de destruction de vos périphériques anciens ou obsolètes, notamment de vos clés USB et de vos disques durs externes ?

Si de surcroît votre entreprise détient des informations, des données ou des protocoles hautement confidentiels

12. Interdisez-vous strictement toute connexion à des périphériques ?
13. Utilisez-vous des périphériques chiffrés *(mot de passe, code PIN, certificat électronique, carte à puce token USB, bio-reconnaissance…)* ?
14. Utilisez-vous un logiciel de protection *(antivirus)* pour l'utilisation des périphériques ?
15. Utilisez-vous un logiciel de connexion sécurisé des périphériques ?
16. Utilisez-vous un isolateur USB ?
17. Placez-vous un boîtier de désactivation du clavier entre le port USB et le périphérique ?
18. Utilisez-vous des jetons USB ?
19. Utilisez-vous une clé USB ou un disque dur externe pour manipuler les données présentes sur un ordinateur isolé du réseau et de toute connexion à Internet *(Air gap)* ?

Explications

Un périphérique informatique est un dispositif connecté à un système d'information central *(ordinateur, console de jeux, etc.)* auquel il permet d'ajouter des fonctionnalités.
Les périphériques sont soit « d'entrée », c'est-à-dire qu'ils servent à fournir des informations ou des données au système informatique *(ce sont les claviers, les souris, les scanners, les micros, les webcams, etc)* soit « de sortie », c'est-à-dire qu'ils servent à faire sortir des informations du système *(ce sont les écrans, les imprimantes, les haut-parleurs, etc.)*.

Il existe également des périphériques « d'entrée-sortie », comme les lecteurs-enregistreurs de CD-ROM, les disques durs externes, les clés USB etc.
Un périphérique est « local » lorsqu'il est branché directement sur l'ordinateur.

Il est « réseau » lorsqu'il est branché à un réseau informatique avec un ordinateur central ou un serveur.
Sur les micro-ordinateurs, tous les périphériques sont reliés à la carte-mère, soit connectés dans un port *(port USB)* soit dans un port *(USB)* disponible sur une carte d'extension, elle-même enfichée sur la carte-mère.

Le système d'exploitation installé sur le système informatique doit disposer d'un pilote pour le périphérique, *un driver*.

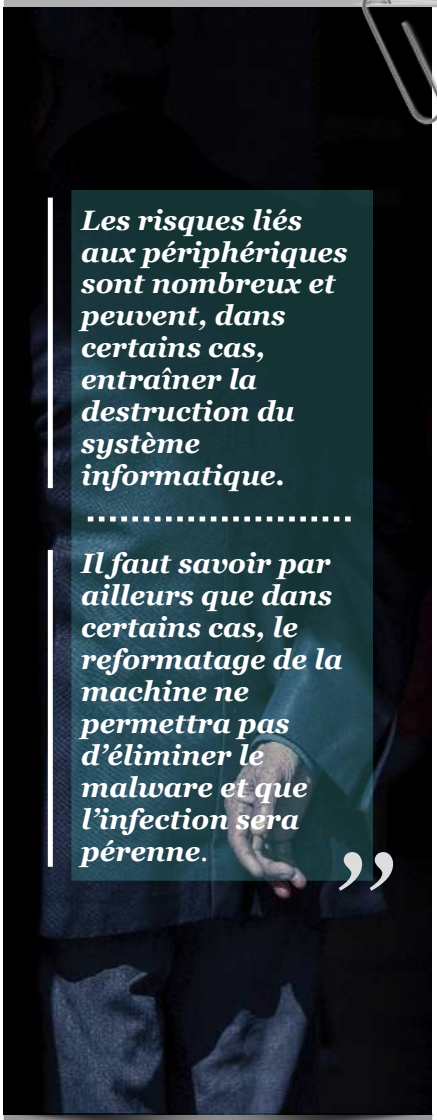
> ***« Les périphériques USB doivent être considérés comme un vecteur d'attaques potentiel »***

C'est un logiciel chargé de communiquer avec lui et d'intégrer ses fonctionnalités au système d'exploitation.

Aujourd'hui la norme USB *(Universal Serial Bus ®)* s'est universalisée et constitue à travers le monde le mode de connexion des périphériques le plus répandu, voire le seul.

C'est dans ce cadre que dès 2011 les chercheurs réunis à la conférence *Black Hat* considéraient que c'est l'ensemble des périphériques USB qui doivent être considérés comme un vecteur d'attaques potentielles.

Les réseaux informatiques se montrant de plus en plus résistants aux attaques, c'est à présent par les médias amovibles, et particulièrement par l'intermédiaire des clés USB, que sont perpétrées les infections : la sécurité USB est aujourd'hui devenue un enjeu majeur et primordial de la sécurité informatique.



Les risques liés aux périphériques sont nombreux et peuvent, dans certains cas, entraîner la destruction du système informatique.

Il faut savoir par ailleurs que dans certains cas, le reformatage de la machine ne permettra pas d'éliminer le malware et que l'infection sera pérenne.

1. Les risques liés aux périphériques

Que l'ordinateur soit éteint ou allumé, et même si l'antivirus est à jour, ces risques peuvent être :

- la copie des saisies clavier
- l'écoute des claviers
- la simulation de frappe
- la copie des mots de passe
- la copie des données
- l'extraction de toutes données et de tous codes
- l'injection d'applications indésirables
- l'injection de logiciels malveillants
- l'infection par cheval de Troie
- l'infection par vers *(worms)*
- les propositions frauduleuses de streaming
- l'introduction de « logiciels rançon »
- la destruction de la carte-mère

1. Les risques liés aux périphériques

« Voici quelques exemples à connaître, donnant une bonne idée des risques que peuvent représenter les périphériques »

BAD USB

Il est indétectable par l'antivirus. Une fois installé, il opère, que l'ordinateur soit allumé ou éteint. Il utilise une faille commune à tous les ordinateurs, et pour ce faire n'importe quel périphérique USB. Il procède par reprogrammation du firmware *(micro logiciel intégré d'origine permettant le fonctionnement d'un système informatique)*, et ce faisant, permet au matériel infecté d'évoluer grâce aux mises à jour. Ainsi le firmware ouvre l'accès à n'importe quel virus souhaité par le cyber-attaquant.

USB KILL

Il provoque la destruction de l'ordinateur en « grillant » la carte mère par surtension. La clé branchée, munie de condensateurs qui se chargent via la tension du port USB *(5 volts)*, se décharge brutalement par fractions de secondes en libérant 110 volts sur le port USB, détruisant ainsi jusqu'à 95% de la machine. Une nouvelle génération de USB Killer a très vite vu le jour. Dite « USB Killer V2 », elle libère 220 volts en continu.

POISON TAP

Il exploite la confiance des ordinateurs envers les périphériques réseau. Il profite de cette confiance pour se faire passer pour une nouvelle connexion Ethernet avec priorité haute, en vue d'intercepter le trafic.

En moins d'une minute :

- il ouvre une backdoor *(porte de derrière)* permanente.
- puis il récupère les cookies et s'approprie les différents comptes et les mots de passe.

WIRELUKER

Il est conçu pour infecter les terminaux APPLE et les périphériques iOS branchés sur un port USB. Toutes les données d'un iPhone deviennent alors accessibles. Il faut noter qu'en dehors de Wireluker, des logiciels espions peuvent infecter les smartphones lors de leur connexion *(via l'interface USB)* à des bornes de rechargement publiques. Le logiciel espion s'installe à l'insu de la victime.

Il permet :

- d'établir des communications téléphoniques
- d'envoyer des sms
- de récupérer les contacts de la carte SIM
- de modifier le code PIN
- de récupérer les fichiers contenus sur la carte SD
- d'injecter des malwares

1. Les risques liés aux périphériques

« Un autre vecteur d'attaque qui se situe au niveau de l'activation de ADB (Androïd Debug Bridge) permet :

- *de bénéficier des droits de super-utilisateur*
- *d'installer des applications non certifiées*
- *de désinstaller des applications*

Il est aujourd'hui possible d'espionner des ordinateurs non connectés en utilisant des émetteurs-récepteurs radio dissimulés dans des connecteurs USB d'apparence classique et qui ont été insérés dans les ordinateurs par l'intermédiaire du fabricant ou d'un espion, ceci dans un rayon de treize kilomètres. Il ne faut pas oublier qu'aujourd'hui des éléments de mémoire peuvent être dissimulés dans un chewing-gum ou dans une dent, qu'ils sont difficilement détectables aux portiques de sécurité et qu'ils peuvent ensuite être introduits dans des locaux et connectés.

USBee

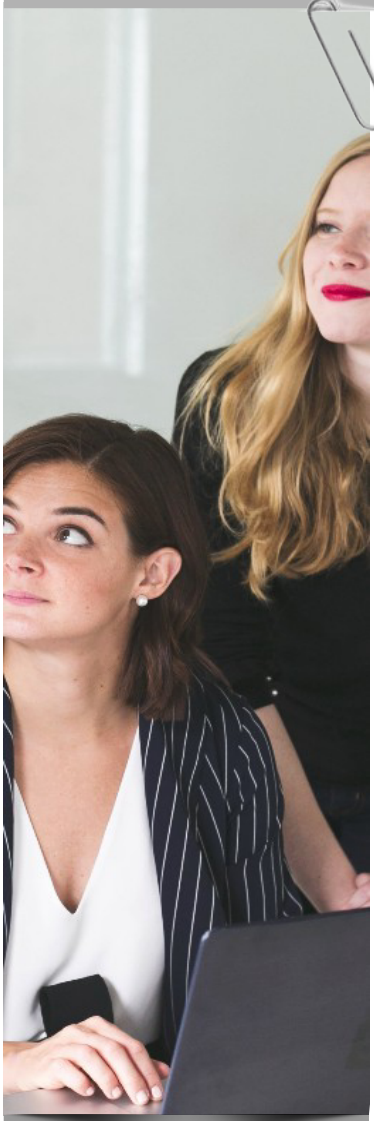
Il permet de voler des données provenant d'ordinateurs isolés en air gap en infectant la machine par connexion à une clé USB. *(un air gap, aussi appelé air wall, est une mesure de sécurité consistant à isoler physiquement un système à sécuriser de tout réseau informatique. Cette mesure, lorsqu'elle est correctement implémentée, rend toute tentative de piratage à distance impossible, quelle que soit sa sophistication.)*

STUXNET

C'est un ver qui une fois installé :
- Espionne et reprogramme les systèmes industriels *(principalement les produits Siemens)*.
- **Attention :** il sait dissimuler les modifications qu'il apporte.

LOCKY

C'est un cheval de Troie crypto-verrouilleur. Il est diffusé par courrier électronique et se présente sous la forme d'une pièce jointe qui doit être ouverte avec Microsoft Word. Le fichier Word attaché contient un texte qui indique d'activer les macro-définitions pour pouvoir lire le texte. Ce fichier copié sur une clé USB reproduit les mêmes effets à son ouverture. Une fois LOCKY installé à l'insu de la victime, il :
- Supprime les ponts de restauration quand Windows effectue des mises à jour *(cela rend toute restauration à l'état antérieur impossible)*
- Chiffre les disques physiques et les périphériques USB
- Chiffre également le partage réseau ? *(serveur de fichiers)*, alors que c'est à cet emplacement que se trouve toute l'intelligence collective d'une société
- Indique une rançon à payer pour obtenir un code de déchiffrage dont l'efficacité n'est pas prouvée. »



2. Les contre-mesures logicielles

Il faut ici parler plus de contre-mesures que de solutions. Il n'existe pas véritablement de solution sûre et définitive.

La prévention en la matière pourrait se résumer en une pratique et en une phrase :

RETENEZ BIEN CECI !

"il faut informer, former, inculquer les bonnes pratiques et les appliquer de manière draconienne.

Pour ne pas se faire piéger, seule la vigilance finit par payer."

3. Les contre-mesures matérielles

- L'utilisation des « jetons USB carte à puce » permet un accès pratique et sécurisé aux réseaux d'entreprise et aux services Internet, en fournissant une authentification forte. Les applications et les données restent sur le jeton, ce qui permet d'avoir une empreinte zéro sur l'hôte.

- « Plug DB » est une clé USB qui contient une carte mémoire chiffrée par des clés cachées sur une puce et qui dispose d'un capteur d'empreinte digitale. Aucun pilote n'est nécessaire, car tout se trouve dans la clé.

- Il existe également des capteurs biométriques.

- Le boîtier « USB Shield », qui se place entre le port USB et la clé USB, désactive la fonction clavier ce qui bloque toute attaque « Bad USB ».

- Il existe des isolateurs USB qui fonctionnent sans alimentation, et peuvent résister à une tension allant jusqu'à 2000 volts sur la ligne USB.

4. Les contre-mesures comportementales

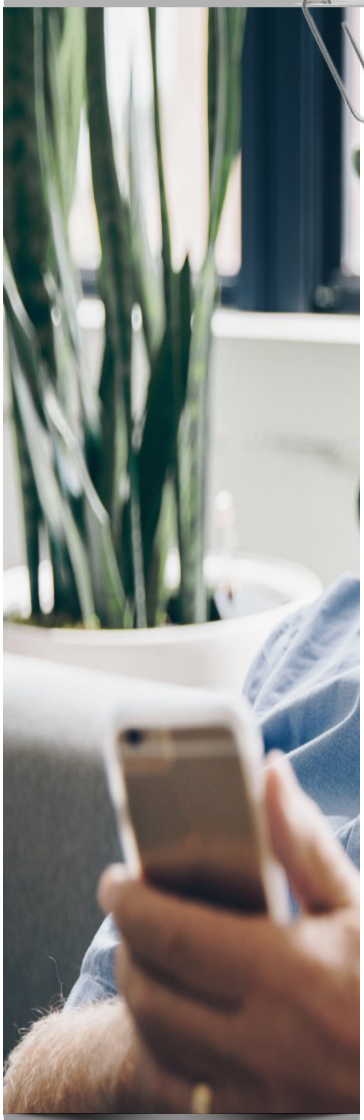
Il ne faut jamais :

- *utiliser une clé USB, ou un disque dur, trouvés par hasard*
- *utiliser une clé USB, ou un disque dur, offerts*
- *utiliser une clé USB, ou un disque dur, d'une marque inconnue*
- *recharger son téléphone à une borne publique*

Il faut :

- *faire analyser par l'antivirus les fichiers présents sur la clé USB ou le disque dur*
- *désactiver l'exécution automatique des supports amovibles depuis l'ordinateur*
- *désactiver physiquement les ports USB lorsque leur utilisation n'est pas nécessaire*
- *désactiver les périphériques de démarrage dans le BIOS [1] et protéger l'accès à celui-ci par un mot de passe*

[1] Le Basic Input Output System - BIOS, en français : système élémentaire d'entrée/sortie - est, au sens strict, un ensemble de fonctions, contenu dans la mémoire morte (ROM) de la carte mère d'un ordinateur, lui permettant d'effectuer des opérations de base lors de sa mise en route.



Réalisons un questionnaire test

1. Votre entreprise a-t-elle un « pare feu reverse » *(firewall)*, qui sécurise votre réseau informatique, contrôlant les flux et les applications entrantes et sortantes ?
2. Y a-t-il des procédures standardisées de mise à jour des logiciels filtres ?
3. Avez-vous un mot de passe sécurisé pour la connexion au réseau ?
4. Le compte Administrateur a-t-il une adresse IP et un mot de passe différent du compte Utilisateur ?
5. L'accès au serveur est-il dans un local sécurisé ?
6. L'hébergeur de votre système de messagerie est-il sécurisé *(anti-spam, antivirus, chiffrement TLS…) ?*
7. Chaque utilisateur a-t-il un mot de passe sécurisé pour utiliser sa messagerie *(réception et envoi)* ?
8. Avez-vous établi des consignes de sécurité standardisées lors de la réception des courriels ?
9. Avez-vous formé vos employés à ces consignes de sécurité ?
10. Avez-vous un réseau dédié pour communiquer avec vos partenaires ?
11. Pour vos recherches, avez-vous un ordinateur dédié qui est différent du poste Administrateur ?
12. Vos recherches sur Internet se font-elles en mode privé ?
13. Avez-vous des procédures standardisées pour utiliser des sites web lors de vos recherches ?
14. Avez-vous formé vos employés à ces procédures de recherche ?
15. Lors de l'utilisation du wi-fi, votre entreprise a-t-elle pris des mesures de sécurité ?

1. La connexion internet

“Le Web... & Explications Solutions...

Le web relie les ordinateurs de l’entreprise entre eux *(via un serveur intranet)*

et/ou

Relie certains ou tous les ordinateurs au réseau mondial d’Internet *(extranet)* avec tous ses services, ses vulnérabilités et sa sécurité.

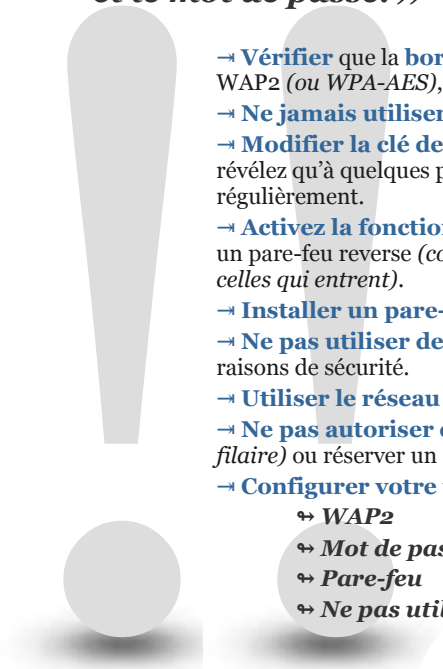
Chaque serveur possède une adresse IPv4 *(Internet Protocol version 4)*, de notation décimale à points :

les différents niveaux de réseaux :

- **le WEB que nous utilisons quotidiennement**
- **le WEB profond que nous utilisons dès notre identification avec un mot de passe**
- **le WEB caché illégal ”**

Sécurisez sa connexion internet...

> ***La borne d'accès à Internet c'est la box. Cet accès peut se faire par le wi-fi ou par une installation filaire*** *(qui est plus sécurisée mais moins pratique).*
> ***Il est nécessaire de configurer votre borne d'accès en modifiant l'identifiant de connexion et le mot de passe.***



- **Vérifier** que la **borne d'accès** dispose d'un protocole de chiffrement WAP2 *(ou WPA-AES)*, qu'il faut activer.
- **Ne jamais utiliser le WEP**, très facile à casser en 2 minutes.
- **Modifier la clé de connexion** par un mot de passe, que vous ne révélez qu'à quelques personnes de confiance, et que vous changez régulièrement.
- **Activez la fonction pare-feu** de votre box, l'idéal étant de procéder à un pare-feu reverse *(contrôle des connexions qui sortent mais aussi de celles qui entrent)*.
- **Installer un pare-feu et un antivirus** sur votre ordinateur.
- **Ne pas utiliser de wi-fi public** *(gare, aéroport, hôtel...)* pour des raisons de sécurité.
- **Utiliser le réseau VPN**.
- **Ne pas autoriser de clients** à se connecter sur votre réseau *(wi-fi ou filaire)* ou réserver un accès dédié
- **Configurer votre wi-fi**
  - ***WAP2***
  - ***Mot de passe sécurisé***
  - ***Pare-feu***
  - ***Ne pas utiliser de wi-fi public, sauf si WPN***

2. La messagerie

(les mails, les courriels...)

"Les courriels et pièces jointes sont les principaux facteurs d'attaque informatique. C'est la porte d'entrée de votre maison, les issues de secours, les portes fenêtres...

Faites en sorte que l'on ne puisse en aucun cas ni entrer ni sortir."

• Choisir un hébergeur du système de messagerie sécurisée :

• Il doit disposer d'un antivirus

• Il doit disposer de cryptage Transport Layer Security (TLS) ou Sécurité de la couche de transport lors des échanges serveurs/utilisateurs *(reverse)*

• Il doit disposer d'un service anti spams

• Choisir son mot de passe *(Cf. mot de passe)*

• Distinguer le compte professionnel du compte personnel

• Les questions à se poser avant d'ouvrir un mail :

• L'expéditeur est-il connu ?

• Une information de sa part est-elle attendue ?

• Le lien ou le sujet est-il cohérent avec le sujet évoqué ?

• Méthode de vérification de manière générale :

• Utiliser un autre canal *(SMS, téléphone... en utilisant un annuaire connu avec test secret)*

• Ne pas ouvrir le mail en cas de doute

• Si des liens figurent dans un courriel, passer la souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur et vous permettra de vérifier la cohérence

• Ne pas transférer un mail professionnel vers la boîte mail professionnelle et vice versa

• Ne pas ouvrir les spams

• Ne pas ouvrir la pièce jointe de manière automatique, sans lancer une analyse antivirus

• Ne jamais répondre par courriel si l'on vous demande des informations personnelles *(numéro de carte bancaire, numéro de téléphone, adresse personnelle...)* même si l'expéditeur est un site officiel *(banque, impôts, assurance, ministère...)*

• N'ouvrir, ni ne relayer aucun message en chaîne *(même s'il s'agit d'une alerte antivirus, ou chaîne de solidarité...)*

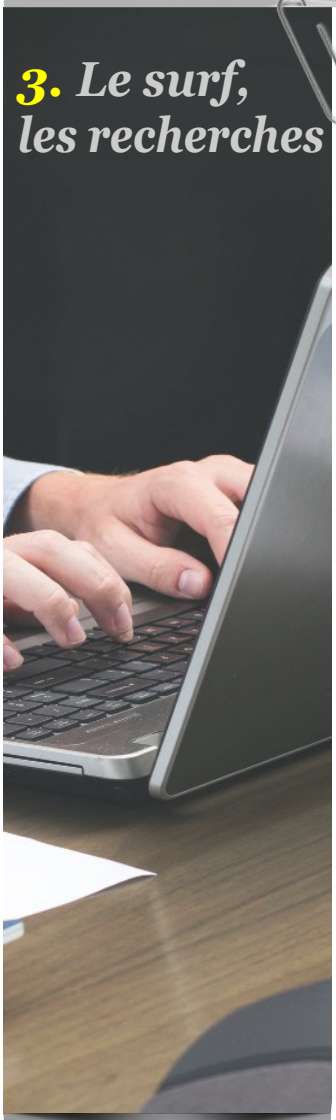
• Réseau dédié entre partenaires :

• Établir une connexion privée

• Ou établir un tunnel de site à site type Internet Protocol (IP)*

** est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique.*

3. Le surf, les recherches



Pour le poste de travail Administrateur :

- Pas d'accès Internet *(toute contamination de ce poste entraînerait une contamination de tous les autres postes)*
- Réserver à l'Administrateur un ordinateur dédié pour ses recherches ou communications en ligne
- Effectuer les mises à jour sur le poste Administrateur, hors ligne, sur site officiel, sur support amovible, après contrôle infection, puis transférer hors ligne
- Cloisonner ce poste Administrateur : l'installer dans une pièce différente de celle de l'Utilisateur, cryptage IPsec tunnel *(Internet Protocol Security)*, choix d'un réseau local virtuel, communément appelé VLAN *(pour Virtual LAN)* différent de celui du poste en Utilisateur.

Pour tous les postes :

- Navigation privée : pas de sauvegarde du mot de passe en fin de session, pas de mémoire de l'historique des recherches, pas de cookies
- Pas de clic intempestif sur n'importe quel sujet
- Pas d'ouverture de pièce jointe sans réfléchir et sans analyse par antivirus
- Pas d'ouverture des fenêtres et bandeaux publicitaires *(pop-up)*
- Lors des recherches : utilisation des sites S *(sécurisé)*, type HTPPS, avec cadenas

4. Le World Wide Web dit "Web"

Votre site web est la vitrine de votre entreprise.

Il peut vous permettre de toucher des personnes que vous n'auriez pas rencontrées. Il vous permet de présenter vos services ou de proposer vos produits en vous créant ainsi, l'opportunité d'élargir votre clientèle.

L'hébergeur de votre site Web met à votre disposition un espace via **un serveur** qui doit être sécurisé comme tout serveur *(voir plus haut)*.

Il s'occupe de la gestion du matériel et des serveurs.

Vous, vous êtes responsable des données que vous y mettez : site web, e-mail, fichiers...Vous devez contrôler cet espace.

Les serveurs de votre hébergeur doivent être **sécurisés** et disposer d'outils permettant de bloquer certains comportements suspects.

Les hébergeurs sont des professionnels qui ont la maîtrise de leurs outils. Après une attaque, ils suspendent votre site. A vous de corriger le problème.

Les attaques sont en règle générale d'origine humaine.

Elles ont pour but soit d'effacer votre site soit de le défigurer à des fins concurrentielles soit de l'utiliser à une autre fin *(politique ou autre)* soit de le remplacer.

Sécuriser son site Web permet de :

- protéger les données *(les vôtres ou celle de vos clients)*,
- renforcer la confiance du visiteur vis-à-vis de votre site,
- améliorer le référencement.

Depuis janvier 2018, le moteur de recherches Google™ affiche le message *« non sécurisé »* à côté de l'adresse des sites qui utilisent le protocole HTTP. De plus, il référence de manière privilégiée les sites utilisant HTTPS.

Si vous proposez à vos clients un paiement en ligne, la loi vous oblige à utiliser un protocole HTTPS avec certificat SSL *(échange sécurisé entre navigateur et serveur)*.

Sécuriser votre site Web en HTTPS (S pour sécuriser)

Cela permet de vérifier l'identité de votre site, et de garantir que les échanges sont cryptés du début à la fin.

Cela permet également de sécuriser les pages que vous visionnez et que vous renseignez.

Installer un SSL

C'est un fichier à installer à côté de votre site internet sur votre site d'hébergement.

Il permet :

- d'identifier le propriétaire du site
- de crypter
- de sécuriser les communications entre serveur et visiteur *(mot de passe, carte bancaire..)*, au travers d'un protocole sécurisé HTTPS.

- **Mettre à jour la sécurité de votre site régulièrement**
- **Changer régulièrement votre mot de passe sécurisé**
- **Sauvegarder et protéger vos données sensibles**
  (chiffrer vos données et votre connexion SSL)
- **Vérifier la sécurité de votre hébergeur**

À l'extérieur de l'entreprise

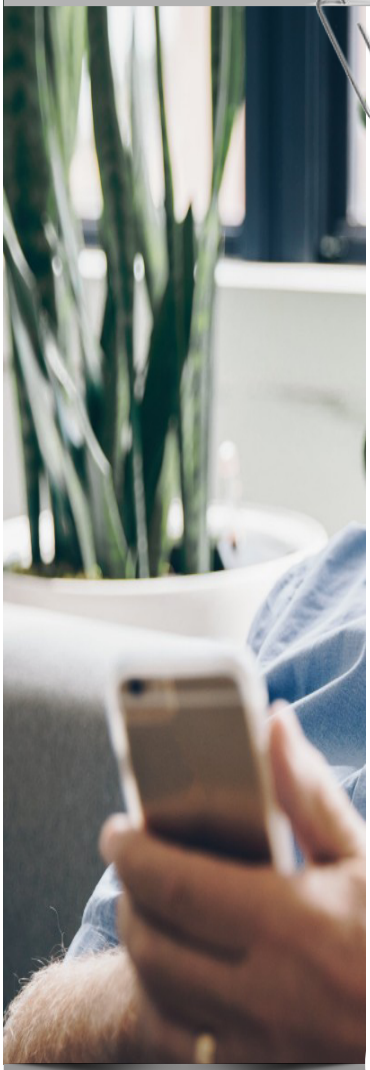
A – DANS LES TRANSPORTS

B – EN VOYAGE, EN SÉJOUR

C – DANS LES SALONS & CONGRÈS

D – À LA MAISON, EN PRIVÉ

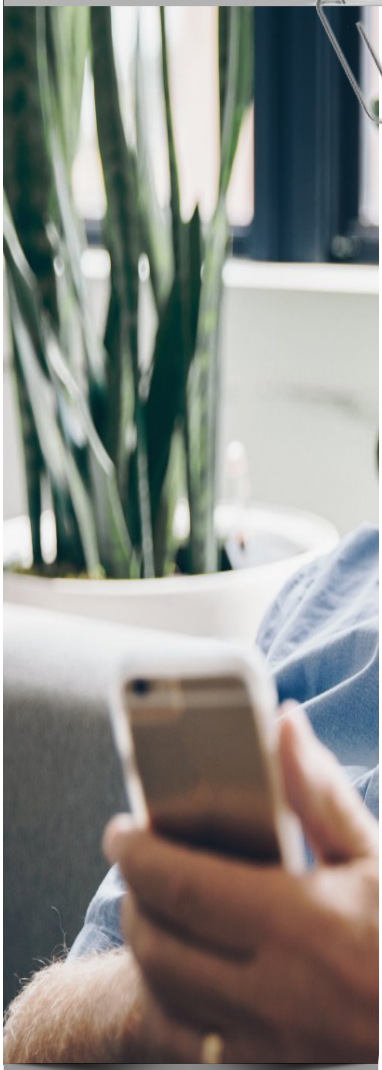
A - Dans les transports



Réalisons un questionnaire test

Avez-vous établi des règles de bon usage pour protéger les informations à l'extérieur de votre entreprise ?

A - Dans les transports



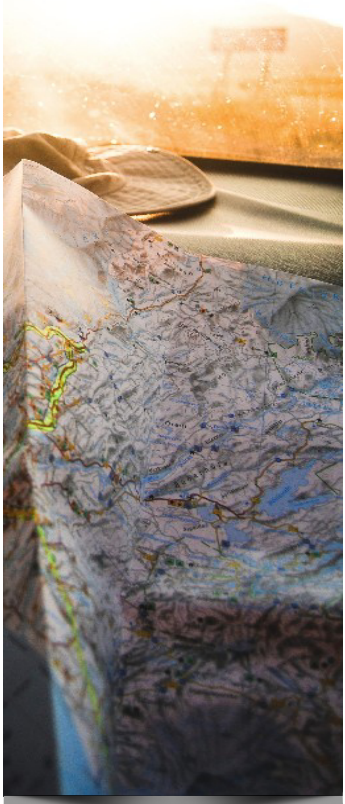
1. Éviter de parler au téléphone *(train, avion…)* ou de vive voix de sujets professionnels
2. Ne jamais recharger son téléphone et son ordinateur sur un port USB public ou mis à disposition
3. Ne jamais se connecter sur un port USB non sécurisé ou inconnu
4. Éviter d'utiliser les moyens de communication mis à disposition *(hôtel, gare, avion, taxi, transports en commun …)*
5. Désactiver le wi-fi, la géolocalisation…
6. Mettre en œuvre une solution de communication sécurisée entre l'utilisateur nomade et le réseau de l'entreprise *(VPN – réseau privé virtuel)*
7. Sélectionner les documents à transporter
8. Surveiller les outils de travail *(mallette, ordinateur, tablette, téléphone)*, même pour des arrêts courts *(coffre de voiture…)*
9. Ne jamais laisser, même dans un coffre-fort, des documents sensibles

souvenez-vous !

B - En voyage, en séjour

Explications & solutions

« Quels que soient les pays et quel que soit leur régime politique, dans un grand nombre d'entre eux, les centres d'affaires et les réseaux téléphoniques sont surveillés. Par ailleurs, dans certains pays, les chambres d'hôtel sont « visitées » à votre insu »



Avant de partir :

• **Consultez** le site du ministère des affaires étrangères : https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/ pour prendre connaissance de la législation locale

• **Consultez** les recommandations préconisées sur le site de l'Agence nationale de la sécurité des systèmes d'information (A.N.S.S.I)

• **Assurez-vous** que les appareils que vous emportez contiennent uniquement les informations dont vous avez besoin pour votre mission

• **Évitez** si possible de partir avec des données sensibles

• **Mettez** en place un système de récupération de fichiers chiffré sur votre lieu de mission.

  • Soit en accédant au réseau de votre entreprise par une liaison sécurisée

  • Soit en utilisant une boîte de messagerie en ligne spécialement créée et dédiée au transfert de données chiffrées *(après lecture, les données doivent être supprimées de la boîte)*

• **N'emportez** que du matériel dédié aux missions *(ordinateurs, tablettes, téléphones, supports amovibles etc.)*

• **Sauvegardez** les données que vous emportez et placez la sauvegarde en lieu sûr

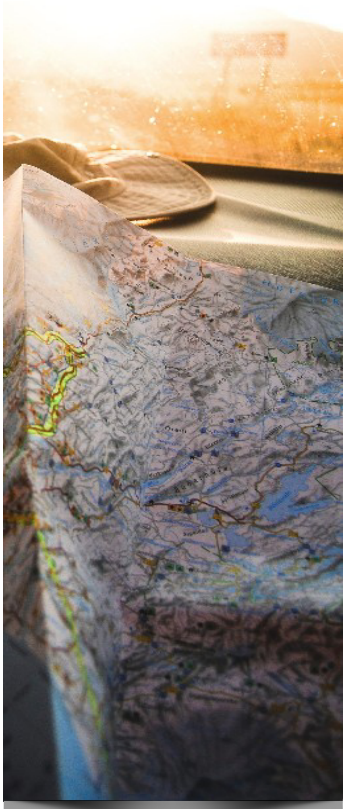
B - En voyage, en séjour

Explications & solutions

« Les cybercafés, les hôtels… et généralement tous les lieux publics, en France comme à l'étranger, n'offrent aucune garantie de confidentialité.

Une fois arrivé sur le lieu de votre déplacement, vous serez plus vulnérable que d'ordinaire, même si vous êtes en terrain connu.

Vous devez être particulièrement vigilant. »



● Durant le voyage :

• Ordinateur, tablette, téléphone, supports amovibles : **ne les laissez jamais** dans un bureau, dans votre chambre d'hôtel, même dans le coffre-fort de votre chambre d'hôtel, quand vous vous absentez

• Si vous devez vous séparer de vos équipements informatiques, **conservez** avec vous la carte SIM ainsi que la batterie

• **Ne communiquez pas** d'information confidentielle en clair par téléphone ou tout autre moyen de transmission de la voix *(Skype™ par exemple)*

• **Effacez l'historique** de vos appels et de vos navigations internet *(historique, données en mémoire cache, cookies, mots de passe d'accès, fichiers temporaires…)*

• **Méfiez-vous** des rencontres fortuites ou supposés fortuites, comme des retrouvailles…

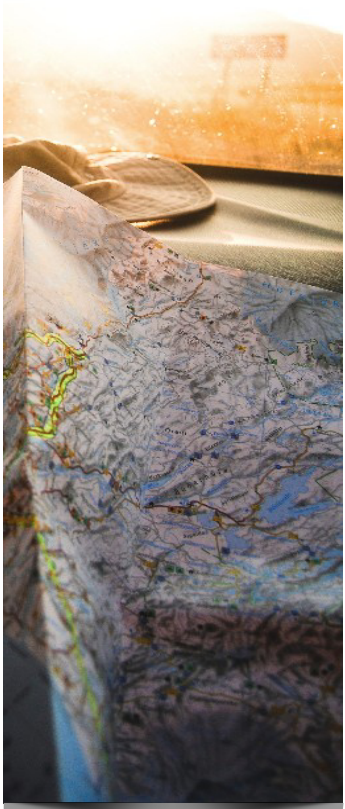
• **N'utilisez pas** les équipements *(notamment les clés USB)* qui vous sont offerts ou qui sont mis à votre disposition

• **Ne rechargez jamais** vos équipements sur les bornes électriques en libre-service

• **Ne procédez pas** à des photocopies sur place

B - En voyage, en séjour

Explications & solutions



● *Avant de rentrer de voyage :*

> ***“ Avant de quitter le lieu de votre mission, il s’agit de transférer à votre entreprise les données qui sont nécessaires, puis, en quelque sorte, de couper les ponts derrière vous. ”***

• **Transférez** vos données à votre entreprise de manière chiffrée puis effacez-les de votre équipement de façon sécurisée *(logiciel prévu à cet effet)*

• **Effacez** l’historique de vos appels et de vos navigations

● *De retour de voyage :*

> ***“ Là encore, vous devez prendre un certain nombre de précautions avant de pouvoir utiliser à nouveau vos équipements et surtout de les reconnecter au réseau ”***

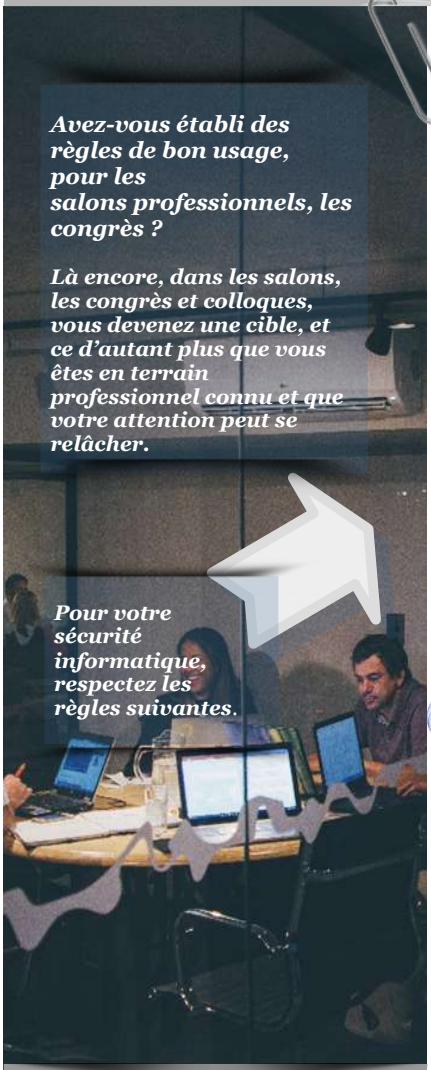
• **Changez** tous les mots de passe que vous avez utilisés durant votre voyage

• **Faites analyser** vos équipements

• **Ne connectez** pas vos équipements à votre réseau avant d’avoir fait un test antivirus et anti-espiogiciel

souvenez-vous !

C – Dans les salons & congrès



Avez-vous établi des règles de bon usage, pour les salons professionnels, les congrès ?

Là encore, dans les salons, les congrès et colloques, vous devenez une cible, et ce d'autant plus que vous êtes en terrain professionnel connu et que votre attention peut se relâcher.

Pour votre sécurité informatique, respectez les règles suivantes.

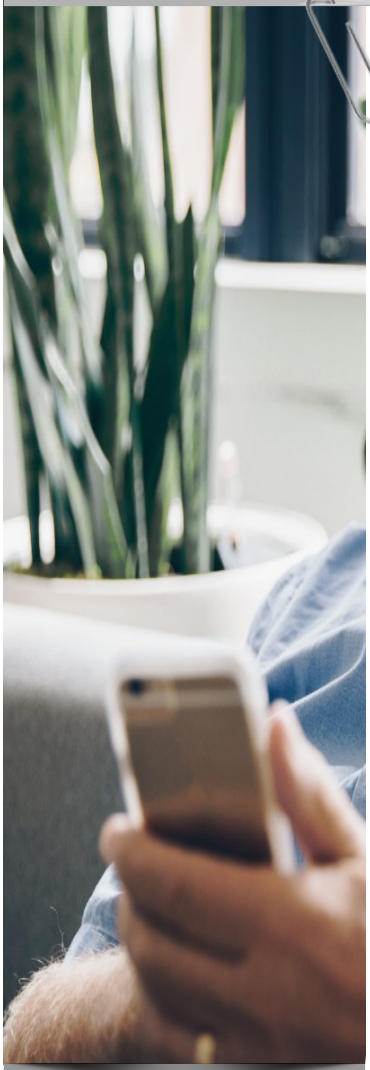
- Assurez-vous que les appareils que vous emportez contiennent uniquement les informations dont vous avez besoin pour votre mission
- Évitez si possible de partir avec des données sensibles
- Utilisez du matériel dédié à ce type de mission
- Méfiez-vous des rencontres fortuites et sympathiques, comme des retrouvailles
- Dans vos conversations, livrez uniquement les renseignements utiles, privilégiez l'écoute
- N'utilisez pas les équipements *(notamment les clés USB)* qui vous sont offerts ou qui sont mis à votre disposition
- Ne connectez jamais vos équipements à des postes ou des périphériques qui ne sont pas sûrs
- Emportez une clé destinée aux échanges d'informations *(présentations, exposés, etc.)*, et détruisez-la après usage
- Ne rechargez jamais vos équipements sur les bornes électriques en libre-service
- Au retour, changez tous les mots de passe que vous avez utilisés durant votre voyage
- Au retour, faites analyser vos équipements
- Ne connectez pas vos équipements à votre réseau avant d'avoir fait un test antivirus et anti-espiogiciel
- Ne faites pas de photocopies sur place

RETENEZ BIEN CECI !

1. Anticipez les objectifs, les informations à diffuser et à collecter
2. Surveillez le matériel à risque durant le salon, restez vigilant dans les conversations *(privilégiez l'écoute)*
3. Sécurisez l'échange de données
4. Méfiez-vous des rencontres fortuites
5. Rédigez un document de synthèse à la fin, avec débriefing des faits surprenants *(contacts…)*
6. Refusez les cadeaux *(USB, objets connectés…)*
7. Ne vous connectez jamais sur un port USB non sécurisé ou inconnu

souvenez-vous !

D – À la maison, en privé



Réalisons un questionnaire test

“Avez-vous établi des règles de bon usage pour vos employés lorsqu’ils sont à la maison ?”

1. Ne pas faire suivre les messages électroniques professionnels sur la messagerie personnelle

2. Ne pas héberger de données professionnelles sur des équipements personnels *(USB, smartphone, tablette…),* ou sur les moyens de stockage en ligne

3. Inversement, ne pas connecter de support amovible personnel sur du matériel professionnel

4. Être vigilant sur les réseaux sociaux en ne donnant pas de renseignement professionnel confidentiel, ni trop personnel

5. Décocher les cases qui permettent la conservation ou le partage des données

6. Utiliser plusieurs adresses mail *(banque, achat, jeux, forum, réseaux sociaux…)* avec mots de passe différents et sécurisés

D – À la maison, en privé

Explications & solutions

- ***Chez vous, vous devez être d'autant plus vigilant que votre attention est relâchée ; vous êtes en « mode détente ».***
- ***Veillez à votre identité 3.0***

Tout ce que vous mettez sur les réseaux sociaux est stocké et peut mettre en péril votre entreprise soit en exposant le sujet de votre travail dans un domaine concurrentiel soit en dégradant votre réputation personnelle.
Par ailleurs, méfiez-vous des rencontres sur la toile.

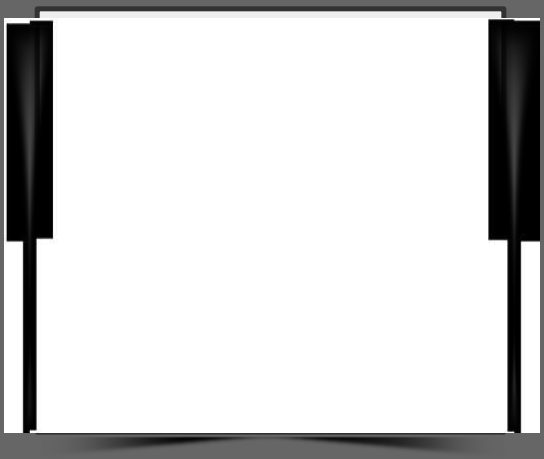
RETENEZ BIEN CECI !

identité numérique

- Cloisonner au maximum le privé et le professionnel
- Ne pas transférer de messages professionnels sur sa boîte privée et inversement
- Ne pas connecter de support amovible sur son ordinateur privé et inversement
- D'une manière générale, ne pas héberger de données professionnelles dans un espace privé
- Ne jamais parler de ce qui relève de la sphère professionnelle sur les réseaux sociaux
- Rester discret sur les réseaux sociaux quant aux informations qui vous sont personnelles
- Dans les formulaires à remplir, décocher les cases qui permettent la conservation ou le partage des données
- Utiliser plusieurs adresses mail *(banque, achat, jeux, forum, réseaux sociaux…)* avec mots de passe différents et sécurisés

souvenez-vous !

Lexique



Certaines de ces définitions concernent des notions ou des vocables simples mais dont le contenu ou les contours nous sont parfois flous.

D'autres sont relatives à des éléments plus complexes et vous permettront soit d'assouvir votre curiosité soit de disposer d'un support lors de vos lectures sur le sujet soit dans le pire des cas, de cerner la difficulté que vous rencontrez au sein de votre entreprise.

A

Adresse IP

Une adresse IP *(avec IP pour Internet Protocol)* est le numéro qui identifie chaque ordinateur connecté à Internet, ou plus généralement et précisément, l'interface avec le réseau de tout matériel informatique *(routeur, imprimante)* connecté à un réseau informatique utilisant l'Internet Protocol.

ADSL

Protocole de transmission numérique à haut débit qui utilise le réseau téléphonique.

A.N.S.S.I. : Agence nationale de la sécurité des systèmes d'information

L'A.N.S.S.I. est un service rattaché au Secrétaire général de la défense et de la sécurité nationale (S.G.D.S.N.), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. L'A.N.S.S.I. apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (O.I.V.). Elle est chargée de la promotion des technologies, des produits et services de confiance, des systèmes et des savoir-faire nationaux auprès des experts comme du grand public. Elle contribue ainsi au développement de la confiance dans les usages du numérique. Son action, auprès de différents publics, comprend la veille et la réaction, le développement de produits pour la société civile, l'information et le conseil, la formation ainsi que la labellisation de produits et de prestataires de confiance.

Air gap – (ou Air wall)

En sécurité informatique, un air gap, aussi appelé air wall, est une mesure de sécurité consistant à isoler physiquement un système à sécuriser de tout réseau informatique. Cette mesure, lorsqu'elle est correctement implémentée, rend toute tentative de piratage à distance impossible, quelle que soit sa sophistication.

A

Antivirus
Logiciel capable de détecter les virus informatiques et de les éliminer.

Androïd
Android est le système d'exploitation mobile créé par Google™. Il équipe la majorité des téléphones portables du moment *(smartphones)*. Son principal concurrent est Apple™ avec l'Iphone™. ... Android est réputé pour être plus libre et ouvert que iOs, le système qui équipe l'iPad d'Apple.

Assistant
(Voir « Wizard ».)

B

Backdoor
Un programme backdoor *(littéralement porte arrière mais traduit par porte dérobée)* est un petit bout de code introduit en général par un pirate informatique pour pouvoir ouvrir un accès dérobé sur un système informatique et ainsi prendre le contrôle de celui-ci quand il le désire.

BadUSB
Il est indétectable par l'antivirus. Une fois installé, il opère, que l'ordinateur soit allumé ou éteint. Il utilise une faille commune à tous les ordinateurs, et pour ce faire n'importe quel périphérique USB.
Il procède par reprogrammation du firmware *(micro logiciel intégré d'origine permettant le fonctionnement d'un système informatique)*, et ce faisant, permet au matériel infecté d'évoluer grâce aux mises à jour. Ainsi le firmware ouvre l'accès à n'importe quel virus souhaité par le cyber-attaquant.

BIOS
Le Basic Input Output System *(BIOS, en français : « système élémentaire d'entrée/sortie »)* est, au sens strict, un ensemble de fonctions, contenu dans la mémoire morte *(ROM)* de la carte mère d'un ordinateur, lui permettant d'effectuer des opérations de base lors de sa mise sous tension, par exemple l'identification des périphériques d'entrée/sortie connectés et la lecture d'un secteur sur un disque. Par extension, le terme est souvent utilisé pour décrire l'ensemble du micro-logiciel de la carte mère. C'est en quelque sorte le centre de contrôle de la carte mère.

B

Bit

Le bit est l'unité la plus simple dans un système de numération, ne pouvant prendre que deux valeurs, désignées le plus souvent par les chiffres 0 et 1. Un bit ou élément binaire peut représenter aussi bien une alternative logique, exprimée par faux et vrai, qu'un chiffre du système binaire.

Boîte de dialogue

En informatique, une boîte de dialogue est un composant d'interface graphique constitué d'une fenêtre affichée par un programme ou par le système d'exploitation soit pour informer l'Utilisateur d'un événement soit pour obtenir une information de l'Utilisateur. Ces fenêtres sont appelées boîte de dialogue parce qu'elles établissent un dialogue entre l'ordinateur et l'Utilisateur.

Bootkit

Est un synonyme de rootkit, parfois simplement « kit », est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès à un ordinateur de la manière la plus furtive possible. Il se lance généralement au démarrage.

C

Carte mère

La carte mère est le composant principal de l'unité centrale. Le rôle de la carte mère est de centraliser et traiter les données échangées dans un ordinateur à l'aide du processeur, qui est fixé dessus. La carte mère gère donc le disque dur, un disque, le clavier et la souris, le réseau, les ports USB.

Carte SD

Le format microSD *(de l'anglais Micro Secure Digital Card)* est une des nombreuses interfaces utilisées dans le monde des cartes mémoire, et c'est aussi une des plus petites. Il s'agit d'une unité de stockage qui utilise de la mémoire flash et qui est dérivé du format Secure Digital.

Carte SIM

Carte à puce insérée dans un téléphone portable, sur laquelle sont stockées les informations concernant la connexion GSM de l'abonné.

C

Charge utile

En informatique, on utilise ce terme au figuré pour désigner la partie du code exécutable d'un virus qui est spécifiquement destinée à nuire *(par opposition au code utilisé par le virus pour se répliquer notamment).*

Cheval de Troie

Un cheval de Troie *(Trojan horse en anglais)* est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'Utilisateur.

Dans la mythologie grecque, l'épisode du cheval de Troie est un événement décisif de la guerre de Troie.
À l'initiative d'Ulysse, des guerriers grecs réussissent à pénétrer dans Troie, assiégée en vain depuis dix ans, en se cachant dans un grand cheval de bois, harnaché d'or, offert aux Troyens. Ce stratagème leur permit de pénétrer dans la place sans être vus, mieux encore en ayant portes ouvertes.

Code PIN

Le code PIN *(Personal Identification Number ou numéro d'identification personnel)* est un code d'identification personnel qui permet de sécuriser l'accès à une carte SIM.

Commandes AT

Les Commandes Hayes, parfois appelées Commandes AT, constituent un langage de commandes développé à l'origine pour le modem Hayes Smartmodem 300. Ce jeu de commandes s'est ensuite retrouvé dans tous les modems produits.

Cookies

Petit fichier déposé sur le disque dur à l'insu de l'internaute, lors de la consultation de certains sites web, et qui conserve des informations en vue d'une connexion ultérieure.

Crypto-ransomware

C'est un logiciel malveillant qui crypte et bloque les fichiers contenus sur un ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer.

D

Darknet

Un darknet est un réseau superposé *(ou réseau overlay)* qui utilise des protocoles spécifiques intégrant des fonctions d'anonymisation. Certains darknets se limitent à l'échange de fichiers, d'autres permettent la construction d'un écosystème anonyme complet *(web, blog, mail, irc).*

Dark Web

Le dark web est le contenu du World Wide Web qui existe sur les darknets[1], des réseaux overlay qui utilisent l'Internet public mais sont seulement accessibles via des logiciels, des configurations ou des autorisations spécifiques.

Deep Web

Le web profond, appelé aussi web caché *(en anglais deep web)* ou *« web invisible » (terme imprécis)* décrit dans l'architecture du web la partie de la toile non indexée par les principaux moteurs de recherche généralistes.

DNS

Le DNS *(Domain Name System)* est un système essentiel au fonctionnement d'Internet. C'est entre autres, le service qui permet d'établir la correspondance entre le nom de domaine et son adresse IP.

Domaine

Un domaine, est un ensemble d'ordinateurs reliés à Internet, qui possèdent une caractéristique commune : *.fr*

E

Ethernet

C'est un protocole de réseau local à commutation de paquets. C'est une norme internationale : ISO/IEC/IEEE 8802-3:2014. Depuis les années 1990, on utilise très fréquemment Ethernet sur paires torsadées pour la connexion des postes clients, et des versions sur fibre optique pour le cœur du réseau.

Extranet

Intranet dont l'accès est étendu à certaines personnes extérieures *(fournisseurs, clients, partenaires...).*

F

Firewall

Un firewall *(ou pare-feu)* est outil informatique *(matériel et/ou logiciel)* conçu pour protéger les données d'un réseau *(protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).*

F

G

H

I

Firmware .....

Dans un système informatique, un firmware *(ou micrologiciel, microcode, logiciel interne, logiciel embarqué ou encore microprogramme)* est un programme intégré dans un matériel informatique *(ordinateur, photocopieur, automate (API, APS), disque dur, routeur, appareil photo numérique, etc)* pour qu'il puisse fonctionner.

Format .....

En informatique, un format de données est la façon dont est représenté *(codé)* un type de données, sous forme d'une suite de bits. Par commodité, on interprète cette suite de bits comme un nombre binaire, et on dit par raccourci que la donnée est représentée comme un nombre. Par exemple, le caractère C est généralement codé comme une suite dont 3 bits sont activés, ce que l'on écrit 0100 0011, soit 67 en décimal.

GSM.....

Norme européenne de téléphonie mobile.

HTML.....

Langage de balisage utilisé pour la création de pages web, permettant notamment de définir des liens hypertextes.

HTTP.....

Protocole de transmission permettant à l'Utilisateur d'accéder à des pages web par l'intermédiaire d'un navigateur.

HTTPS .....

L'abréviation HTTPS signifie littéralement "HyperText Transfer Protocol Secure". Ce "protocole de transfert hypertexte sécurisé" combine le protocole de communication client-serveur, ou HTTP, avec un certificat d'authentification du site exploré.

IMEI .....

IMEI signifie International Mobile Equiment Identity. Ce numéro est une série de 15 à 17 chiffres, inscrit sous la batterie de votre téléphone portable et sur le coffret que vous recevez lors de l'achat du téléphone portable. C'est le numéro d'identité de votre téléphone portable.

I

Interface
Dispositif qui permet la communication entre deux éléments d'un système informatique. Dit aussi hyperlien, ou lien hypertexte, ou lien web, ou simplement lien, est une référence dans un système hypertexte permettant de passer automatiquement d'un document consulté à un document lié.

Internet-iFrame
Est le nom d'une balise HTML qui permet d'intégrer une page HTML au sein d'un autre document HTML. iFrame est un raccourci pour inline frame. La balise iFrame permet notamment d'insérer dans une page web des éléments qui proviennent d'un autre serveur sans que le visiteur en ait conscience.

Internet
Réseau informatique mondial.

Intranet
Réseau informatique exclusivement interne *(à une entreprise, un organisme...),* utilisant les techniques d'Internet.

J

Jeton USB
Un jeton d'authentification *(parfois appelé authentifieur, jeton de sécurité, jeton USB, clé USB de sécurité, jeton cryptographique, carte à puce, token ou encore calculette pour ceux disposant d'un clavier),* est une solution d'authentification forte.

K

Keylogger
Dispositif d'espionnage informatique qui enregistre les suites de touches tapées sur un clavier. Il se situe souvent dans un port USB.

L

Langage
On appelle langage informatique un langage formel non nécessairement Turing-complet utilisé lors de la conception, la mise en œuvre, ou l'exploitation d'un système d'information. Le terme est toutefois utilisé dans certains contextes dans le sens plus restrictif de langage de programmation.

L

Locky

C'est un cheval de Troie crypto-verrouilleur. Il est diffusé par courrier électronique, et se présente sous la forme d'une pièce jointe qui doit être ouverte avec Microsoft Word™. Le fichier Word attaché contient un texte qui indique d'activer les macros-définitions pour pouvoir lire le texte. Ce fichier copier sur une clé USB reproduit les mêmes effets à son ouverture. Une fois LOCKY installé à l'insu de la victime, il : **supprime** les ponts de restauration que Windows **effectue** lors des mises à jour *(cela rend toute restauration à l'état antérieur impossible),* **chiffre** les disques physiques et les périphériques USB, **chiffre également** le partage-réseau *(serveur de fichiers)*, alors que c'est à cet emplacement que se trouve toute l'intelligence collective d'une société, **indique une rançon** à payer pour obtenir un code de déchiffrage dont l'efficacité n'est pas prouvée.

Logiciel

Ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données *(par opposition au matériel).*

M

Macro-Définition

En programmation informatique, une macro-définition ou simplement macro est l'association d'un texte de remplacement à un identificateur, tel que l'identificateur est remplacé par le texte dans tout usage ultérieur. Le plus souvent, on permet également le passage de paramètres syntaxiques.

Malware

Un logiciel malveillant ou maliciel, aussi dénommé logiciel nuisible ou programme malveillant ou pourriciel *(«malware» en anglais)*, est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'Utilisateur dont l'ordinateur est infecté.

Mémoire flash

La mémoire flash est une mémoire de masse à semi-conducteurs ré-inscriptible, c'est-à-dire une mémoire possédant les caractéristiques d'une mémoire vive mais dont les données ne disparaissent pas lors d'une mise hors tension.
Ainsi, la mémoire flash stocke les bits de données dans des cellules de mémoire, mais les données sont conservées en

M

mémoire lorsque l'alimentation électrique est coupée. Sa vitesse élevée, sa durée de vie et sa faible consommation *(qui est même nulle au repos)* la rendent très utile pour de nombreuses applications : appareils photo numériques, téléphones cellulaires, imprimantes, assistants personnels *(PDA),* ordinateurs portables ou dispositifs de lecture et d'enregistrement sonore comme les baladeurs numériques, clés USB. De plus, ce type de mémoire ne possède pas d'éléments mécaniques, ce qui lui confère une grande résistance aux chocs.

Mémoire de masse

En informatique, une mémoire de masse est une mémoire de grande capacité, non volatile et qui peut être lue et écrite par un ordinateur. Il n'y a aucun rapport avec la mémoire vive.

Mémoire morte

Originellement, l'expression mémoire morte *(en anglais, Read-Only Memory : ROM)* désignait une mémoire informatique non volatile *(c'est-à-dire une mémoire qui ne s'efface pas lorsque l'appareil qui la contient n'est plus alimenté en électricité)* et dont le contenu est fixé lors de sa programmation, qui pouvait être lue plusieurs fois par l'Utilisateur, mais ne pouvait plus être modifiée[1].

Mémoire vive

La mémoire vive est la mémoire informatique dans laquelle peuvent être stockées, puis effacées, les informations traitées par un appareil informatique. On écrit mémoire vive par opposition à la mémoire morte.

Modem

Appareil qui convertit des signaux afin de transmettre des données entre ordinateurs par le réseau téléphonique ou le réseau câblé.

N

NTI

Abréviation de « nouvelles technologies de l'information ».

O

OS – L'Operating System

Est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs. Il est appelé en français système d'exploitation.

P

Pare-feu

(Voir « Firewall ».).

Périphérique

Un périphérique informatique est un dispositif connecté à un système d'information central *(ordinateur, console de jeux, etc...),* permettant d'ajouter à celui-ci des fonctionnalités.

Les périphériques sont soit « d'entrée », c'est-à-dire qu'ils servent à fournir des informations ou des données au système informatique *(ce sont les claviers, les souris, les scanners, les micros, les webcams etc, soit « de sortie », c'est-à-dire qu'ils servent à faire sortir des informations du système (ce sont les écrans, les imprimantes, les haut-parleurs, etc...).* Il existe également des périphériques « d'entrée-sortie », comme les lecteurs-enregistreurs de CD-ROM, les disques durs externes, les clefs USB, etc.

Ce périphérique est « local » lorsqu'il est branché directement sur l'ordinateur.

Ce périphérique est « réseau » lorsqu'il est branché à un réseau informatique avec un ordinateur central, ou un serveur.

Pilote

Un pilote informatique, souvent abrégé en pilote, est un programme informatique destiné à permettre à un autre programme *(souvent un système d'exploitation)* d'interagir avec un périphérique. En général, chaque périphérique a son propre pilote.

PoisonTap

PoisonTap profite de la confiance qu'ont les ordinateurs envers les périphériques réseau, et une fois connecté à un port USB de l'ordinateur, se fait passer pour une nouvelle connexion Ethernet avec une priorité haute afin d'intercepter le trafic. Que l'ordinateur soit verrouillé ou non, en moins d'une minute une porte dérobée *(backdoor)* sera installée à l'insu de l'Utilisateur légitime. PoisonTap installe des portes dérobées permanentes dans le cache HTTP et récupère les cookies d'identification afin de s'approprier les différents comptes et mots de passe de la victime.

Pour cela, un navigateur doit être déjà ouvert, le dispositif attend que la page web ajoute un nouveau contenu *(pub, mise à jour, nouvelle page, etc.).* Quand cela se produit, PoisonTap répond en délivrant sa charge utile, c'est-à-dire

son code malveillant, sous forme de IFrame en introduisant des versions modifiées des sites les plus populaires. Les cookies sont ainsi stockés dans la carte microSD du Raspberry Pi Zero, ces informations sont envoyées sur un serveur contrôlé par le hacker. Ces portes dérobées continueront à fonctionner lorsque l'appareil PoisonTap sera débranché, permettant de prendre le contrôle à distance sur le réseau local.

P

Pop-up
Fenêtre qui s'ouvre devant la fenêtre principale sans avoir été sollicitée par l'internaute. Les pop-up affichent souvent des messages publicitaires.

Pourriciel
C'est un logiciel malveillant ou maliciel, aussi dénommé logiciel nuisible ou programme malveillant *(« Malware » en anglais),* qui est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'Utilisateur dont l'ordinateur est infecté.

Programme
Un programme informatique est un ensemble d'opérations destinées à être exécutées par un ordinateur. Un programme source est un code écrit par un informaticien dans un langage de programmation. Il peut être compilé vers une forme binaire, ou directement interprété.

Protocole
Un protocole est une méthode standard qui permet la communication entre des processus *(s'exécutant éventuellement sur différentes machines),* c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

R

RAM
Abréviation de l'anglais « Random Access Memory ». C'est la mémoire vive de l'ordinateur.

Rançongiciel et/ou Ransomware
Un ransomware, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur un ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer. Il existe des crypto-ransomware qui cryptent les données.

R

Raspberry Pi

Le Raspberry Pi est un nano-ordinateur monocarte à processeur ARM conçu par le créateur britannique de jeux vidéo, *David Braben*, dans le cadre de sa fondation Raspberry Pi.
Cet ordinateur, qui a la taille d'une carte de crédit, est destiné à encourager l'apprentissage de la programmation informatique ; il permet l'exécution de plusieurs variantes du système d'exploitation libre GNU/Linux-Debian et des logiciels compatibles. Mais également avec les OS Microsoft Windows : Windows 10 IoT Core et Android Pi.
Il est fourni nu *(carte mère seule, sans boîtier, d'alimentation, clavier, souris, ni écran)* dans l'objectif de diminuer les coûts et de permettre l'utilisation de matériel de récupération. Néanmoins des « kits » regroupant le « tout-en-un » sont disponibles sur le web à partir de quelques dizaines d'euros seulement pour ceux qui le désirent.

RAT

C'est un outil d'administration à distance, plus connu sous son nom anglais Remote Administration Tool ou son abréviation RAT. Ce logiciel informatique permet la prise de contrôle à distance d'un ordinateur.

Réseau

Ensemble des moyens matériels et logiciels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.
Note : Tout ou partie de ces matériels peuvent être considérés comme faisant partie du réseau.

ROM

(Voir « Mémoire morte ».).

Rootkit

Un rootkit *(le nom « outil de dissimulation d'activité » est également utilisé, ainsi que « maliciel furtif » et « trousse Administrateur pirate »),* parfois simplement « kit », est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès *(généralement non autorisé)* à un ordinateur de la manière la plus furtive possible, à la différence d'autres logiciels malveillants. Le terme peut désigner la technique de

dissimulation ou plus généralement un ensemble particulier d'objets informatiques mettant en œuvre cette technique.

Routeur
Outil logiciel ou matériel qui assure le routage des données au sein d'un réseau.

Serveur
Un serveur est généralement un ordinateur plus puissant qu'un ordinateur de bureau habituel. Il est spécialement conçu pour fournir des informations et des logiciels à d'autres ordinateurs qui lui sont reliés via un réseau.

Shadow Copy - Shadow Copy *(aussi connu sous le nom Volume Snapshot Service, Volume Shadow Copy Service, ou VSS)* est une technologie incluse dans Microsoft Windows qui permet d'effectuer des sauvegardes automatiques ou manuelles de fichiers ou de disques, même s'ils sont en cours d'utilisation.

Smartphone
Téléphone mobile possédant des fonctions d'assistant personnel, conçu pour avoir des utilisations variées *(Internet, jeux…)*.

Spyware
Littéralement « logiciel espion ». Type de logiciel destiné à recueillir des informations sur les habitudes des Utilisateurs d'ordinateurs, en particulier celles des internautes.
Si les spywares ne sont a priori pas dangereux pour l'ordinateur, ils constituent clairement une violation de l'espace privé de l'Utilisateur, dans le sens où la plupart d'entre eux agissent à l'insu de ce dernier.

Stuxnet
C'est un ver qui une fois installé espionne et reprogramme les systèmes industriels *(principalement le produits Siemens)*. Il sait dissimuler les modifications qu'il apporte.

Système d'exploitation
En informatique, un système d'exploitation *(souvent appelé OS - de l'anglais Operating System)* est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.

T

Terminal
Désigne un ensemble de périphériques de sortie *(écran…)* ou d'entrée *(clavier, souris…),* en quelque sorte l'extrémité d'un réseau.

Trojan horse
(Voir « Cheval de Troie ».).

Token USB
(Voir « Jeton USB».).

U

Upgrade
Mise à niveau d'un matériel et parfois d'un logiciel.

Upload
Mettre en ligne, télécharger vers un serveur, importer, téléverser.

USB
Type de prise *(port)* permettant de connecter un périphérique à un ordinateur. Aujourd'hui la norme USB *(Universal Serial Bus),* qui s'est universalisée et constitue à travers le monde le mode de connexion des périphériques le plus répandu, voire le seul. Attention : le port USB est le vecteur de nombreuses infections et de nombreuses attaques, dont certaines sont létales pour l'ordinateur.

USBee
Il permet de voler des données provenant d'ordinateurs isolés en Air gap *(un air gap, aussi appelé air wall, est une mesure de sécurité consistant à isoler physiquement un système à sécuriser de tout réseau informatique.*

Cette mesure, lorsqu'elle est correctement implémentée, rend toute tentative de piratage à distance impossible, quelle que soit sa sophistication.), en infectant la machine par connexion à une clef USB.

USBKill
Il provoque la destruction de l'ordinateur en « grillant » la carte mère par surtension. La clé branchée qui est munie de condensateurs qui se chargent via la tension du port USB *(5 volts)* se décharge brutalement par fractions de secondes en libérant 110 volts sur le port USB, détruisant ainsi jusqu'à 95% de la machine.Une nouvelle génération de USB Killer a

très vite vu le jour. Dite « USB Killer V2 », elle libère 220 volts en continu.

USB Shield

C'est un boîtier « USB Shield », qui se place entre le port USB et la clef USB désactive la fonction clavier, ce qui bloque toute attaque « Bad USB ». Il existe aussi des boîtiers résistants aux USB Kills.

V

Ver

Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. L'objectif d'un ver n'est pas seulement de se reproduire. Le ver a aussi habituellement un objectif malfaisant.

Virus

Un virus informatique est un programme écrit dans le but de se propager sournoisement et rapidement à d'autres ordinateurs. Il perturbe plus ou moins gravement le fonctionnement de l'ordinateur infecté.

VPN

VPN signifie réseau virtuel privé *(Virtual Private Network).*
Un VPN est un type de réseau informatique qui permet la création de liens directs entre des ordinateurs distants. Côté fonctionnement, le VPN repose sur la création d'un tunnel *(via un protocole d'encapsulation)* entre les deux ordinateurs.
Bien que distants, ces deux ordinateurs sont alors connectés à un même réseau local, virtuel.

Côté usage, le VPN gratuit ou payant permet à certains Utilisateurs d'accéder à un réseau interne *(celui d'une entreprise par exemple)* tout en restant éloigné géographiquement de ce réseau. Mais le réseau privé virtuel est aussi utilisé pour masquer son adresse IP en se connectant à l'extérieur de son propre réseau local. Le VPN participe alors à renforcer l'anonymat d'un Utilisateur lorsqu'il navigue sur le Web et peut aussi servir à contourner la mise en place de restrictions et de filtrages géographiques.

W

Web

Ensemble des données reliées par des liens hypertextes, sur Internet.

Web 2.0

L'expression « Web 2.0 » désigne l'ensemble des techniques, des fonctionnalités et des usages qui ont suivi la forme originelle du web, www ou World Wide Web, caractérisée par plus de simplicité et d'interactivité *(sociabilité)*. ... le web est perçu comme une plate-forme. L'internaute est co-développeur des applications.

Web 3.0

L'expression Web 3.0 est utilisée en futurologie à court terme pour désigner le Web qui suit le Web 2.0 et constitue l'étape à venir du développement du World Wide Web. Son contenu réel n'est pas défini de manière consensuelle, chacun l'utilisant pour désigner sa propre vision du futur d'Internet.

WIFI

Technique qui permet la communication sans fil entre divers appareils *(ordinateur, périphérique, téléviseur…)* grâce aux ondes radioélectriques.

Wireluker

C'est un virus conçu pour infecter les terminaux Apple et les périphériques iOS branchés sur un port USB. Toutes les données d'un iPhone deviennent alors accessibles.

Il faut noter qu'en dehors de Wireluker, des logiciels espions peuvent infecter les smartphones lors de leur connexion *(via l'interface USB)* à des bornes de rechargement publiques.

Le logiciel espion s'installe à l'insu de la victime. Il permet :
D'établir des communications téléphoniques.

- d'envoyer des SMS,
- de récupérer les contacts de la carte SIM,
- de modifier le code PIN,
- de récupérer les fichiers contenus sur la carte SD,
- d'injecter des malwares.

Un autre vecteur d'attaque qui se situe au niveau de l'activation de ADB (Androïd Debug Bridge) permet :

- d'installer des applications non certifiées,

de bénéficier des droits super-Utilisateur,

- de désinstaller des applications,
- de monter une carte SIM,
- de lire le log cat démarrer une application.

W

Worm
(Voir « Ver »).

Wizard
En informatique, un assistant logiciel *(en anglais Wizard = « sorcier » ou « magicien »)* est un programme qui permet d'automatiser certaines tâches, comme l'installation ou le paramétrage.

WWW
Le World Wide Web *(WWW),* littéralement la « toile *(d'araignée)* mondiale », communément appelé le Web, et parfois la Toile, est un système hypertexte public fonctionnant sur Internet.
Le Web permet de consulter, avec un navigateur, des pages accessibles sur des sites. L'image de la toile d'araignée vient des hyperliens qui lient les pages web entre elles.

X

XML
Langage de structuration de données, utilisé notamment pour la gestion et l'échange d'informations sur Internet. XML est un langage plus puisant que HTML.

Z

Zip
Zip est un format de fichier compressé.

CE *guide* A ÉTÉ RÉALISÉ PAR

l'une des équipes des réservistes citoyens de la gendarmerie de Normandie, groupement de gendarmerie départementale du Calvados,

le chef d'escadron (RC) Véronique ALLALI-ZERAH,
médecin endocrinologue,

le chef d'escadron (RC) Sandrine DELISLE,
responsable de marchés Société Générale
Banque Française Mutualiste,

le chef d'escadron (RC) Katell RICHARD,
consultant en communication,

et le lieutenant (RC) Marc BESNARD,
huissier de justice.

« ***Les concepteurs du « Petit Logiciel Illustré » tiennent à remercier,*** *le général Frédéric Aubanel, commandant adjoint la région de Normandie, commandant le groupement de gendarmerie départementale du Calvados, ainsi que le colonel Bruno Louvet, le colonel Laurent Gérin et le capitaine Sylvain Briand qui ont initié ce projet de la Réserve Citoyenne, et qui l'ont fait vivre avec bienveillance. Nous les remercions pour leur soutien constant, ainsi que pour leurs encouragements et leurs conseils. Nous remercions également pour leur aide et leurs conseils précieux les enquêteurs de la plateforme cyber de la section de recherches de Caen.*
Sans eux, ce petit fascicule n'existerait pas. »

Ce guide, destiné aux personnels des entreprises, a été conçu pour être présenté par un militaire de la Gendarmerie Nationale, pouvant être toutefois accompagné par un réserviste de la gendarmerie.

Il a été validé par la Réserve Cyber et par

Directeur de la publication,
Colonel Christophe Junqua,
Gendarmerie du Calvados,

Conception éditoriale et graphique, mise en page
M. Samuel Bellanger,
Gendarmerie du Calvados,

Rédaction,
Réserve Citoyenne, en appui de la cellule "N-Tech" *(nouvelles technologies)*,
Gendarmerie du Calvados,

Crédit photos,
Libre de droits,
GEND/GGD14

- Édition : Septembre 2020 -

De quoi parlerons nous ?

La cyber-sécurité, au 21ème siècle, est devenue un enjeu majeur pour les entreprises.

Cible privilégiée des attaques numériques, quel que soit sa taille, une PME se doit d'en prendre conscience pour se protéger du risque visant à l'espionner ou à la détruire.

Les cyberattaques coûtent cher, très cher aux entreprises. Elles ont de lourdes conséquences, tant sur le plan de leur santé financière, que sur leur réputation.

A l'origine : l'humain, par malveillance ou simplement par erreur.

Ce guide a pour objectif :

- de vous sensibiliser aux risques et aux conséquences des attaques informatiques
- de vous donner les outils pour lutter contre la majorité de ces attaques, qui sont d'origine humaine (erreurs ou malveillances)
- de vous aider à élaborer votre protocole de sécurité informatique, qui s'appliquera à tous vos collaborateurs, et à vous-même.

Nourri par de nombreuses publications, ce guide est le fruit du travail des hommes et des femmes de la réserve citoyenne en partenariat avec la Gendarmerie Nationale, qui est en première ligne pour recenser et démasquer les auteurs de la cybercriminalité, et au fait des nouvelles techniques des hackers.

Il ne remplace aucunement votre équipe d'informaticiens.

Nous vous proposons, pour débuter, 10 questions pour vous permettre d'évaluer le niveau de sécurité de votre entreprise.

En matière numérique les risques pour l'entreprise sont présents à l'intérieur, comme à l'extérieur de l'entreprise, c'est pourquoi il convient d'envisager ces deux situations.

Pour chaque chapitre, vous trouverez des questions tests, qui vous permettrons d'évaluer vos pratiques, puis des explications, et les solutions proposées.